参考資料

Wi-Fi™ Module Product Training

April, 2012

CONFIDENTIAL

Wi-Fi™ Overview

- **Protocol**
  - Built on the IEEE 802.11 standard
  - Conformance testing performed by the non-profit Wi-Fi Alliance (formed in 1999)
- **Consumer Wi-Fi Growth (2009 - 2010)**
  - 158% growth in Wi-Fi enabled consumer electronics
  - 90% cell phones
  - 3 in 4 consumers considered buying a Wi-Fi enabled device
    - 34% laptops
    - 15% Wi-Fi connected 3-D TVs
- **Embedded Systems**
  - Evangelizes on huge hotspot availability
  - Provides data with ultra-low cost transport

CONFIDENTIAL

Wi-Fi™ Overview

- **Roving Networks' Wi-Fi Solution**
  - Industry's lowest power, complete system-on-module solution
    - 4-uA sleep
    - 30-mA Rx
    - Tx variable depending on PA options
  - Compact surface mount design
  - Quick & simple to integrate
  - Complete TCP/IP solution: no external processor or drivers required
- **Feature Rich, Robust Firmware**
  - Standard build: serial port profile
  - Extensions: WebScan™ & sensor

CONFIDENTIAL

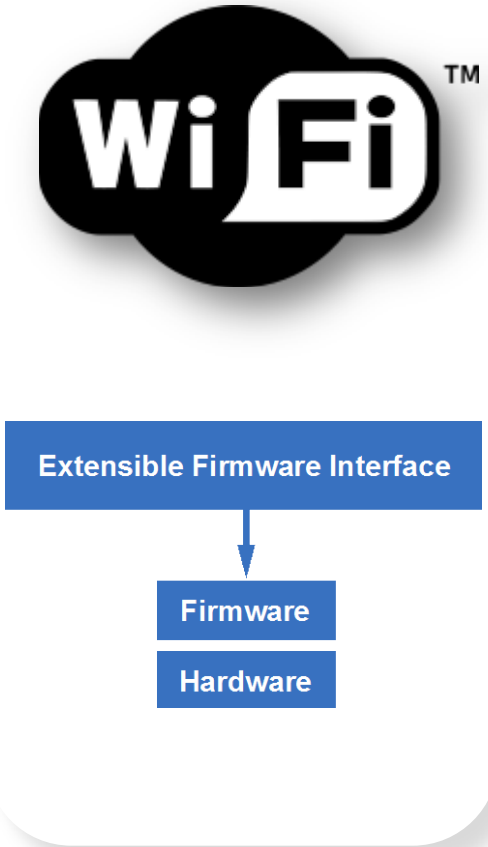
Firmware

April, 2012

CONFIDENTIAL

Roving Networks Firmware

- **Standard Firmware**
  - Simplifies customer design
  - No register-level configurations
  - Manages standard TCP/IP service, e.g., HTTP, DHCP, FTP
- **Firmware Extensions**
  - Builds on the robust, standard firmware
  - Provides application-specific extensions
    - Sensor
      - Remote provisioning
      - Automatic sensor data acquisitions
      - Data logging
    - WebScan™
      - RTLS (Real-Time Location System)



CONFIDENTIAL

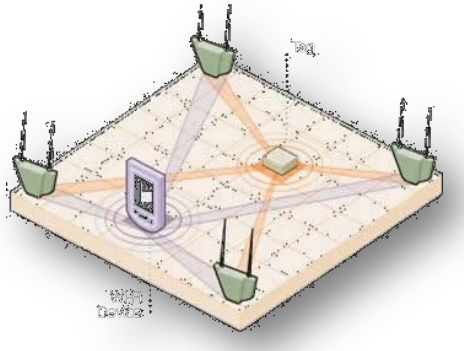
Firmware Extensions

- **Sensor: Real-Time Monitoring**
  - Uses Roving Networks silicon
  - Monitors I/O pin & ADC status
  - Data logger
    - If module disconnects from access point, it stores data until reconnect when data can be sent to server
  - Supports remote provisioning
  - Supports remote software upgrade

CONFIDENTIAL

Firmware Extensions

- **WebScan: Real-Time Location System**
  - Uses Roving Networks silicon
  - Uses I/O pins, ADCs, RFID & timers for wakeup & data generation
  - Measures RSSI levels for triangulation
  - Creates full data packet for server upload

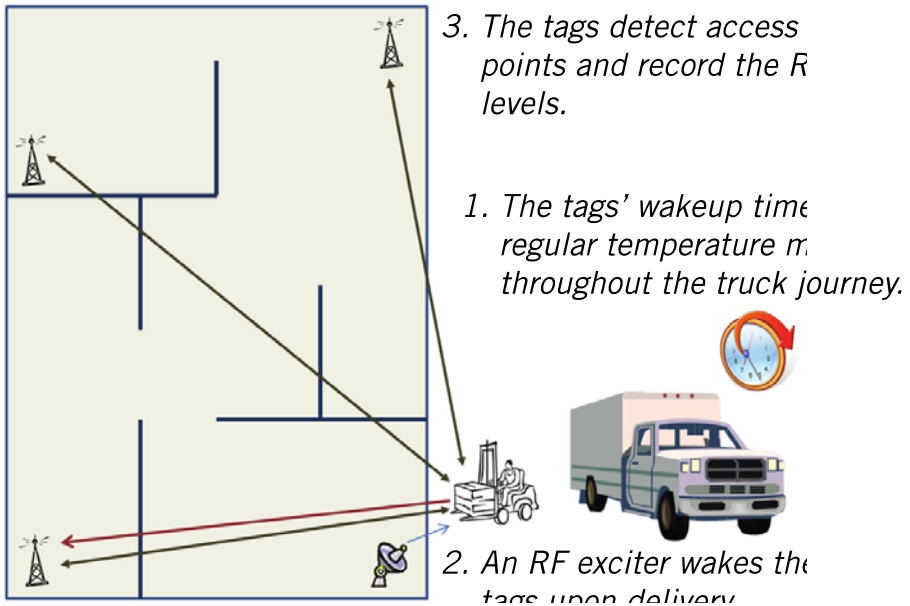


CONFIDENTIAL

Firmware Extensions

• WebScan Example Application

- Goods monitored by tag attached to pallet
- Pallets arrive at docking bay A
- Tag wakes by MAG exciter near docking bay door
- Tag probes for access points & measures their RSSI level
- Tag sends RSSI data to company's server via Wi-Fi
- Tag reports logged data
  - *Refrigeration truck temperatures*
  - *Tag wake up reasons*
  - *Battery life*


3. The tags detect access points and record the R levels.
1. The tags' wakeup time regular temperature m throughout the truck journey.
2. An RF exciter wakes the tags upon delivery

CONFIDENTIAL

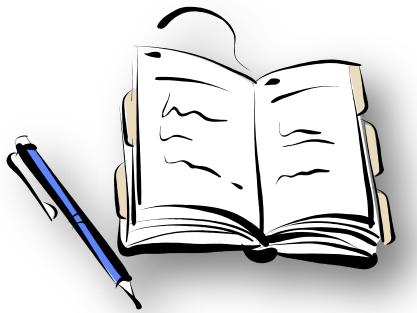
Wi-Fi Lab: Introduction

April, 2012

CONFIDENTIAL

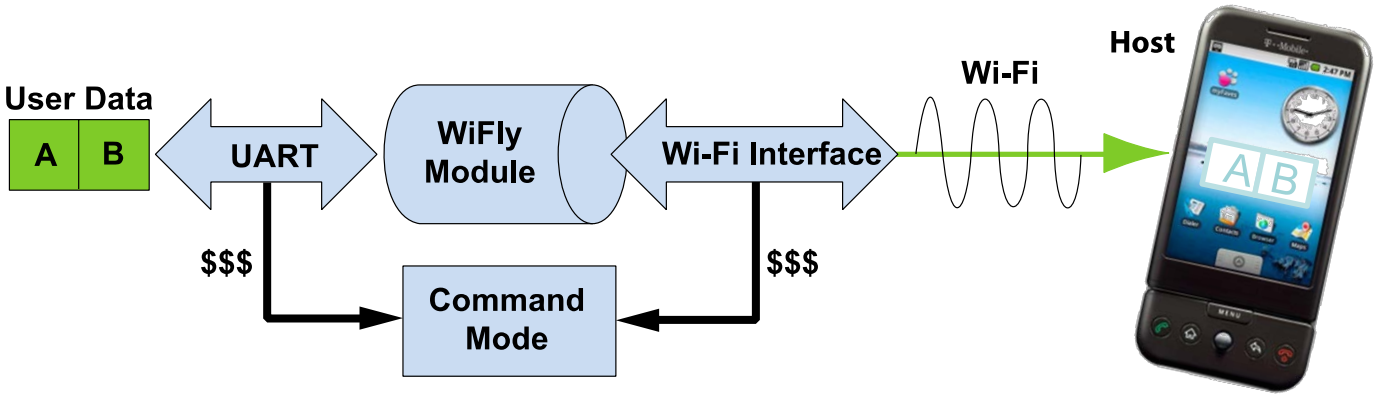
Lab Agenda

- **Introducing WiFly**
  - Firmware
  - Hardware architecture
  - Capabilities
- **Hands-On Wi-Fi Labs**
  - Association & UDP
  - TCP connections & embedded applications
  - Roaming & FTP
  - HTML client & sensors
  - Location tracking (optional)
  - Ad hoc & further FTP (optional)
- **Resources**



CONFIDENTIAL

Data & Command Modes

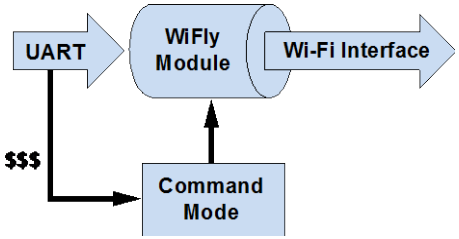


- **Data Mode (Default State)**
  - WiFly module like data pipe
  - TCP/UDP header stripped or added, transparent to UART
  - Data written to UART is sent out over Wi-Fi
  - Data received over Wi-Fi is read from UART
- **Command Mode ($$$)**
  - Special configuration mode entered using $$$
  - Used to assign data, e.g., SSID, pass phrase, etc.

CONFIDENTIAL

Command Mode: Configuration Settings

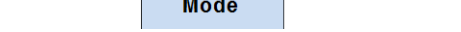
- **Performed Using ASCII Commands**
  - User Guide
- **Configuration Settings Stored in Module's Flash**
  - Changes are persistent & reloaded after power cycling
  - Changes kept using **save** command
  - Many settings require reboot to take effect



CONFIDENTIAL

Command Mode: Syntax

- **Commands Use Keyword Followed by Additional Information**
- **Command Rules**
  - Case sensitive
  - Spaces not allowed, substitute **$**
    “MY NETWORK” = “MY$NETWORK”
- **Can Use Shorthand**
  - set uart baudrate 115200 valid
  - set uart b 115200 valid
  - set u b 115200
    valid
  - s uart baudrate 115200
    Invalid



CONFIDENTIAL

Command Mode: Keywords

- **Set: Immediate Effect, Permanent If Saved to Configuration File**

Set Command	Function
AdHoc	Controls the ad hoc parameters
Broadcast	Controls the broadcast hello/heartbeat UDP message
COMM	Communication & data transfer, matching characters
DNS	DNS host & domain
FTP	FTP host address & login information
IP	IP settings
Option	Optional & infrequently used parameters
Sys	System settings such as sleep & wake timers
Time	Real-time clock settings
UART	Serial port settings such as baud rate & parity
WLAN	Wireless interface, such as SSID, channel & security options

- **Get: Retrieve & Display Permanently Stored Information**
- **Status: Current Interface Status, IP Address, etc.**
- **Action: Perform Actions Such As Scan, Connect & Disconnect**
- **File: Upgrade, Load & Save Configuration, Delete Files, etc.**

CONFIDENTIAL

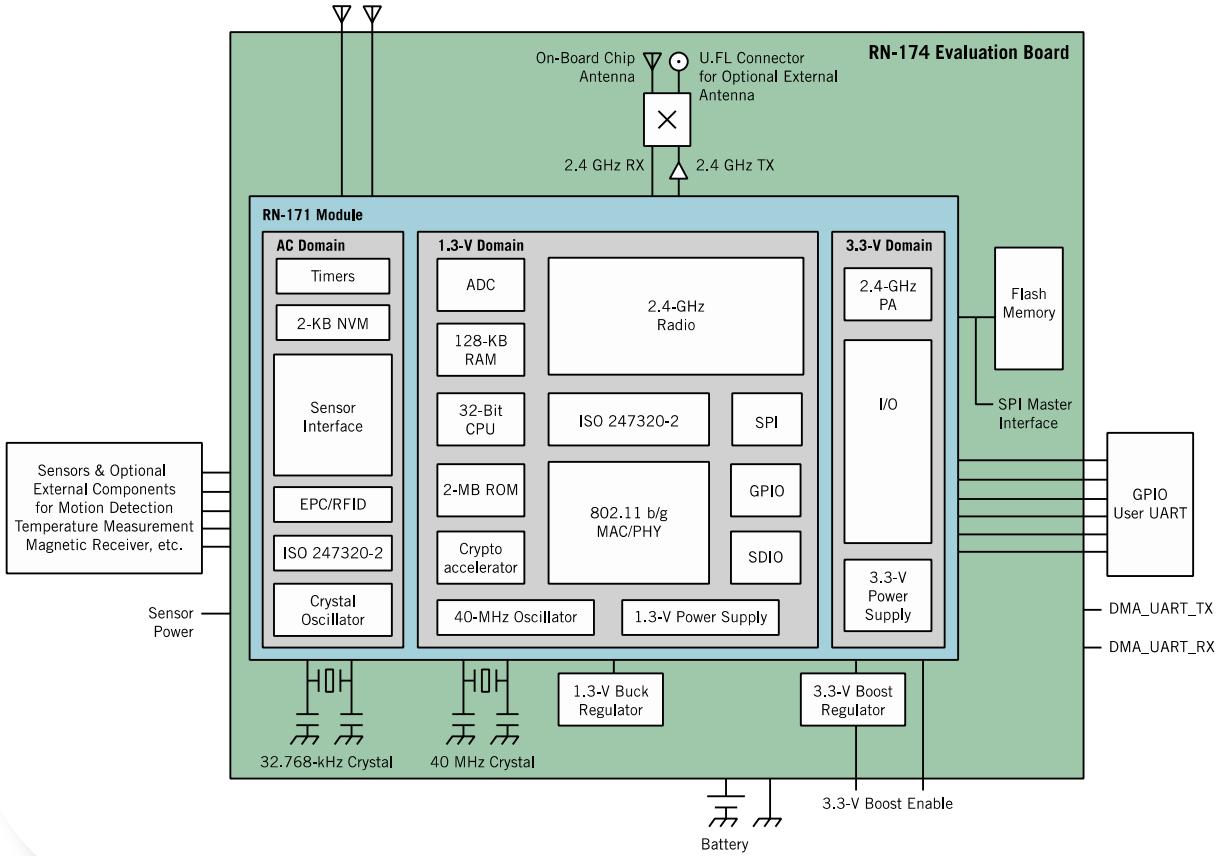
Hardware Architecture: Key Features

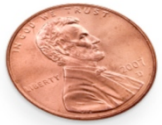
- **2.4-GHz IEEE 802.11b/g Tx/Rx**
- **Ultra Low-Power Consumption**
  - 4-uA sleep
  - 40-mA RX/connected
  - 200-mA maximum TX
- **Sparc 32-Bit Micro**
  - Embedded TCP/UDP/IP stacks
- **Hardware Interfaces**
  - UART: 1-Mbps streaming
  - SPI slave: 2.7-Mbps streaming
- **10 GPIO Pins**
  - Status & control

- **8 Analog Sensor Inputs**
  - 14-bit, 35-us frequency
  - 0 to 1.2 V
- **Security: Hardware Encryption Engine**
  - WEP128
  - WPA-PSK
  - WPA2-PSK (TKIP & AES)
- **Real-Time Clock**
- **1-MB Flash Memory for Data Logging**
- **2-KB NV RAM**
- **Battery Boost Regulator**

CONFIDENTIAL

Hardware Architecture: Silicon





CONFIDENTIAL

Hardware Architecture: Development Environment

RS-232 Interface (J3)

RX - input to evaluation board
TX - output from evaluation board

Pin	Description
1	No connect
2	RS-232 TX
3	RS-232 RX
4	No connect
5	GND
6	No connect
7	RS-232 RTS
8	RS-232 CTS
9	4 to 16 VDC input
10	No connect

Power Select Jumper (J4)

High-Voltage Mode (Default). The board is powered by a source up to 16 V DC.

Low-Voltage Mode. The board is powered by 2.0- to 3.3-V DC only.

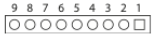
External Power Mode. Used when powering the board with regulated 3.3-V DC power.

GPIO Interface TTL Signals (J8)

RX - input to evaluation board
TX - output from evaluation board

Pin	Description
1	3.3 VDD
2	GND
3	UART RX
4	UART TX
5	GPIO4
6	GPIO5
7	GPIO6
8	GPIO7
9	GPIO8
10	GPIO9
11	UART CTS
12	UART RTS
13	RESET

Sensors (J1)



Pin	Description
1	Sensor PWR
2	Sensor 4 (3.3-V tolerant)
3	Sensor 5 (3.3-V tolerant)
4	Sensor 7 (1.2 V only)
5	Sensor 5 (1.2 V only)
6	Sensor 4 (1.2 V only)
7	Sensor 6 (1.2 V only)
8	Sensor 3 (1.2 V only)
9	GND

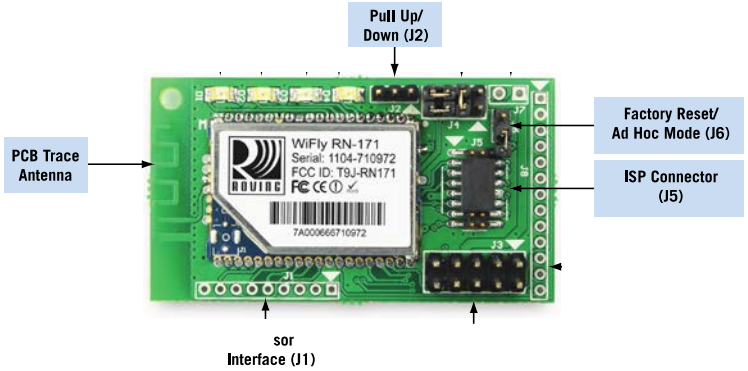
WARNING: Voltage on pins marked *1.2 V Only* should not exceed 1.2 V or permanent damage will occur.

Power (J7)

Pin	Description
1	5 to 12 VDC
2	GND

Pull Up/Down (J2)

Ad Hoc Mode/Factory Reset (J6)



CONFIDENTIAL

Wi-Fi Lab

April, 2012

CONFIDENTIAL

Lab Prerequisites

- **Hardware**
  - RN-134-K or RN-174-K evaluation kit
  - Configured access point (AP)
    - Security: WEP-128, WPA-TKIP or WPA2-AES
  - FTP server to upload & store data
- **Utility Software**
  - Available from http://www.rovingnetworks.com support page
  - Tera Term (terminal emulator)
  - PortPeeker (packet sniffer)

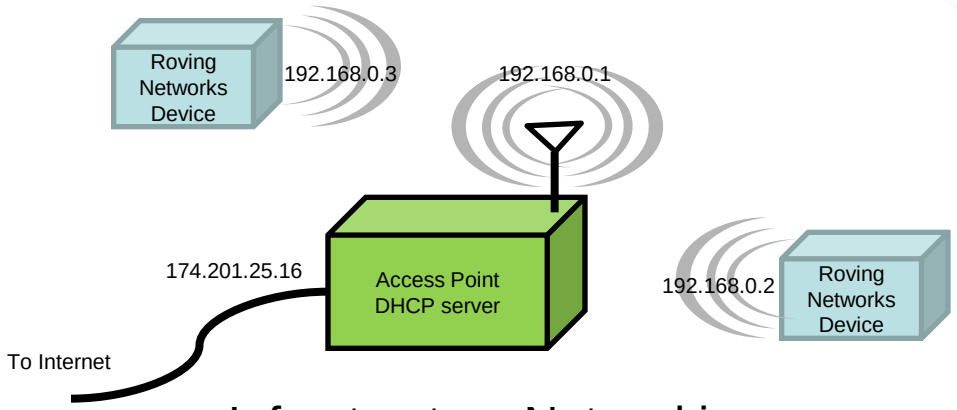
CONFIDENTIAL

Lab 1: Association & UDP

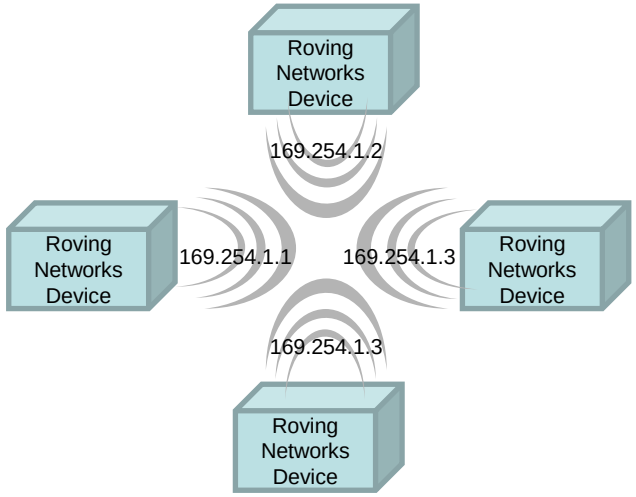
- **Lab Overview**
  - Infrastructure & ad hoc networks
  - Hardware setup
  - Configuration parameters & factory resets
  - Scan, join & authenticate
  - Broadcast UDP
  - Device name
  - Sensor mask
  - UDP auto-pair

CONFIDENTIAL

Lab 1: Association & UDP



Infrastructure Networking



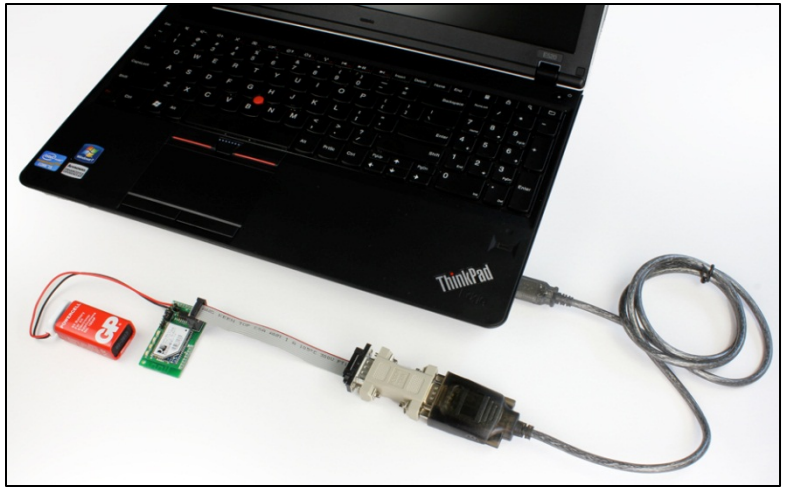
Ad Hoc Networking

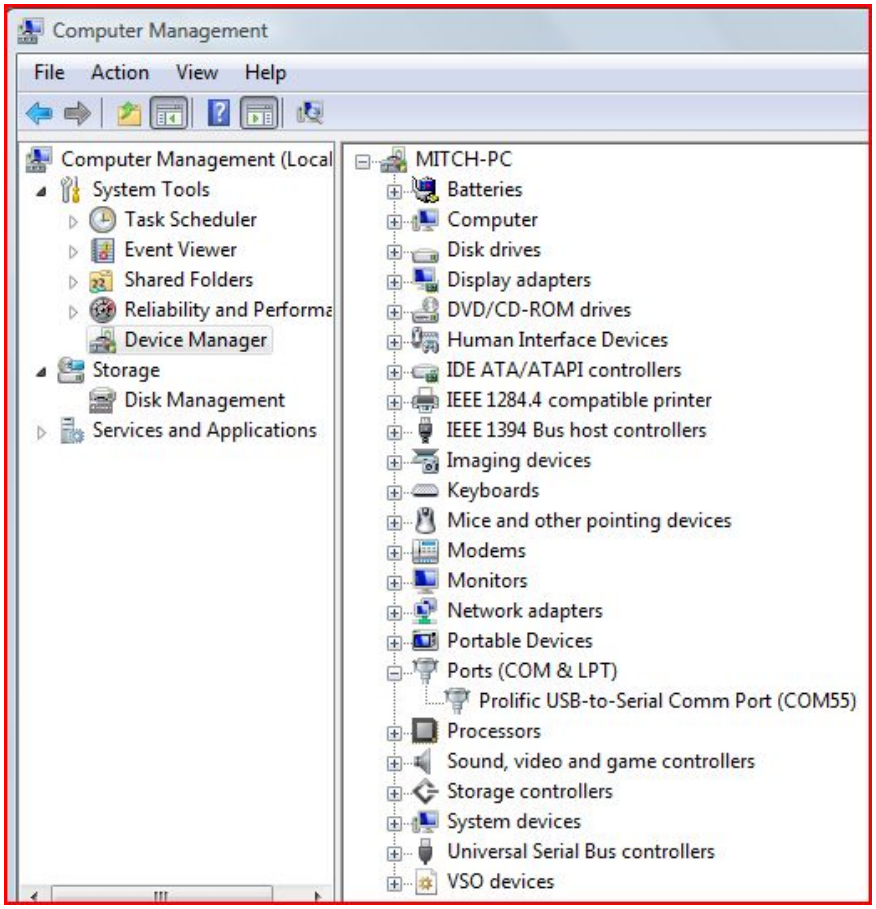
- **Supported Security Modes**
  - WEP 64, WEP 128 **OLD/NOT SECURE**
  - WPA1 TKIP
  - WPA2 AES has not been compromised
  - Enterprise not currently supported
- **Finding Devices on Network**

CONFIDENTIAL

Lab 1: Hardware Setup

- **Connect Evaluation Board**
  - Connect board to your computer
  - Connect battery
    - Blue LED lights up (RN-134-K only)
    - Green LED blinks slowly
  - Use device manager to find the COM port

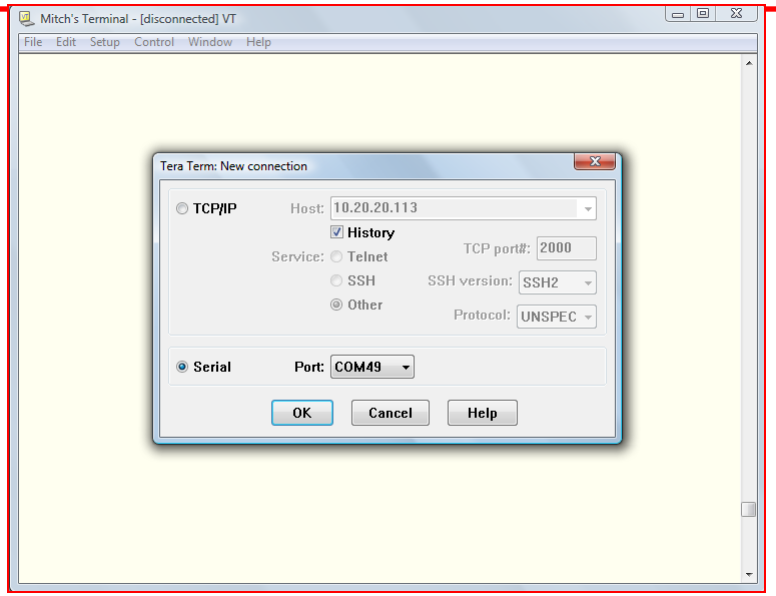




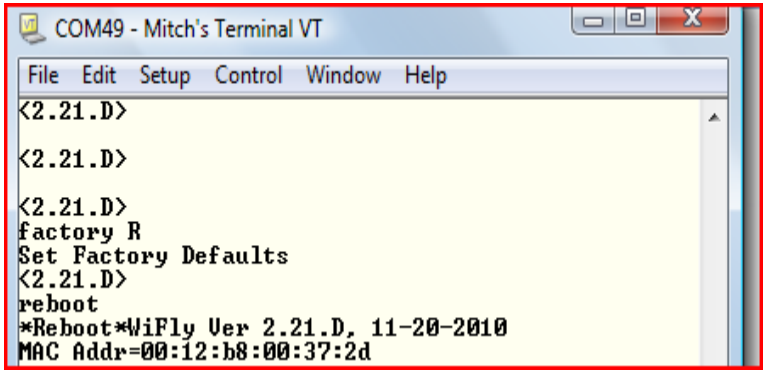
CONFIDENTIAL

Lab 1: Configure Module via UART

- **Launch Command Mode**
  - Run Tera Term
  - Open assigned COM port
    - Serial port settings: 9600 baud, 8 bits, No Parity, 1 stop bit
  - Type **$$$**
  - Module responds with <CMD>



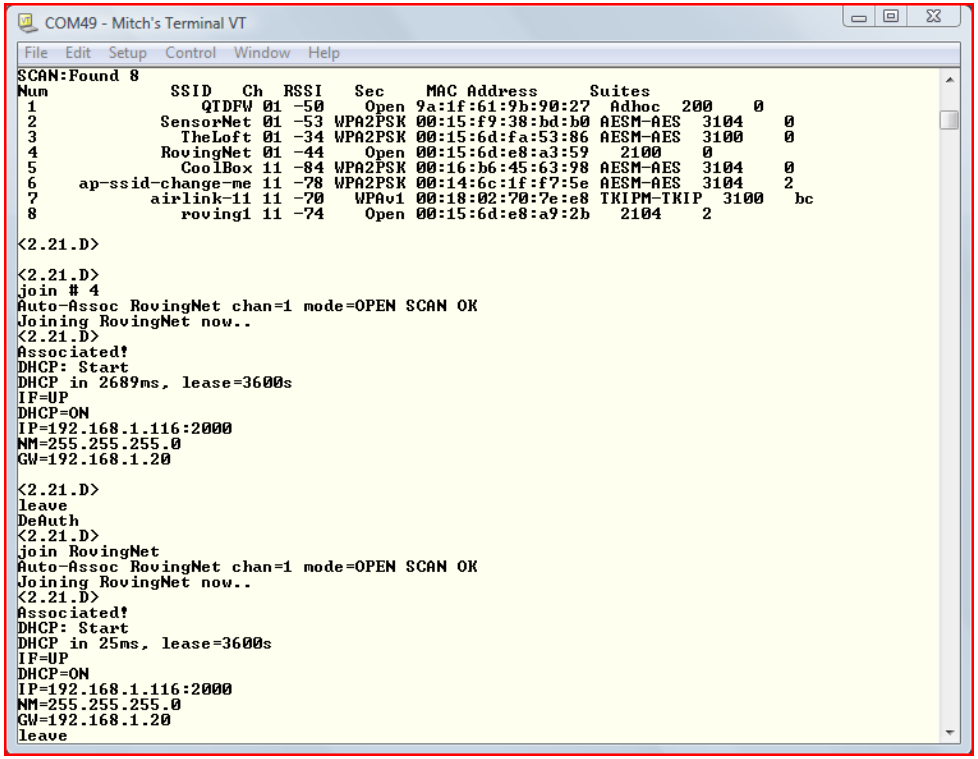
- **Review & Reset Configuration**
  - Check configuration & firmware version
    - **get e**
    - **ver**
  - Perform factory reset (starts module in known state)
    - **factory R**
    - **reboot**



CONFIDENTIAL

Lab 1: Joining/Associating with Networks

- **Search for Networks**
  - **$$$** (enter command mode)
  - **scan**
- **Join a network**
  - **join # 1** (remember spaces)
  - **leave**
  - **join** <*string*> (e.g., **join RovingNET**)
  - **leave**
- **Auto-Join Network with Persistent Configuration**
  - **set wlan ssid** <*string*>
  - **set wlan pass** <*string*>
  - **save**
  - **reboot**

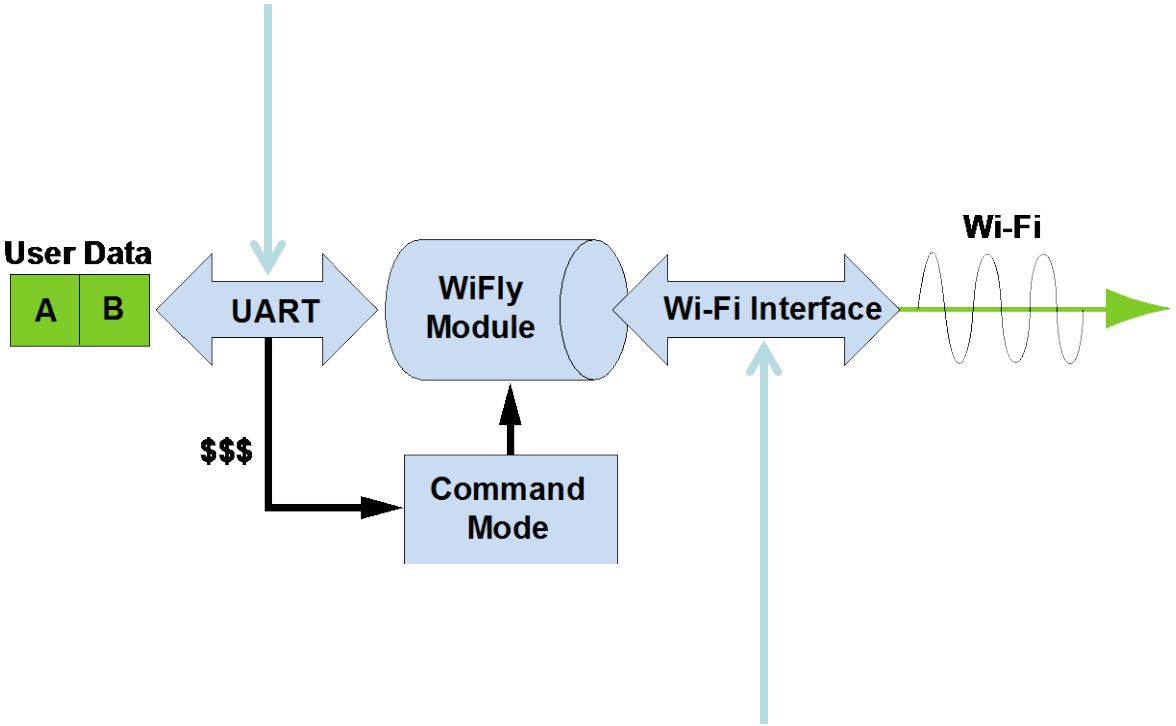


TIP: If Network Is Secure, Set Pass Phrase with set wlan pass <*string*> before Joining Network

CONFIDENTIAL

Lab 1: Interim Summary

- Configured Module via the UART in Command Mode

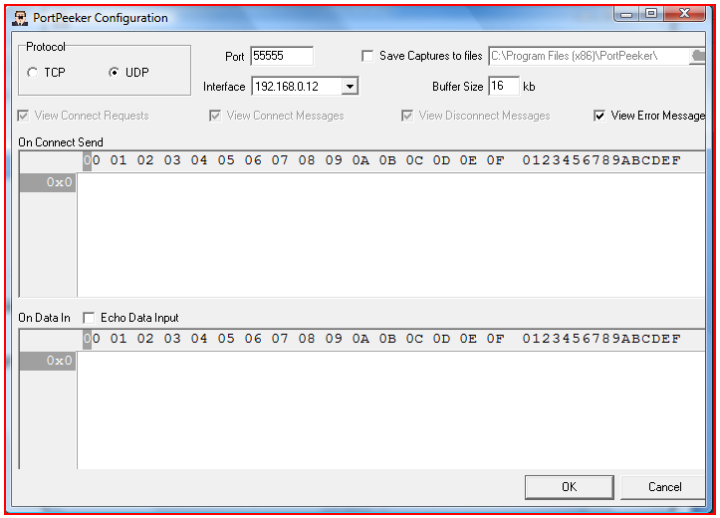


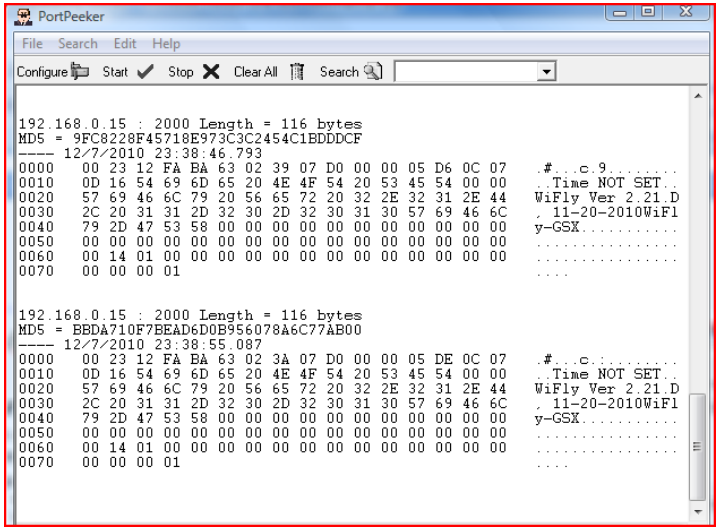
- Next, Observe Wi-Fi Activity Using PortPeeker

CONFIDENTIAL

Lab 1: Configure & Capture UDP with PortPeeker

- **Associate PC with Same AP as Module**
  - Enter command mode & retrieve module's IP address
  - **Ensure PC is on same subnet**
- **Launch & Configure PortPeeker**
  - Click **configure**
  - Set port number to **55555** (default)
  - Set protocol to **UDP**
  - Click **OK**
- **Start UDP Packet Capture**
  - Click **Start**
  - If PC & module are on same subnet, broadcast packets shown
  - If multiple nodes on network, look for YOUR IP address

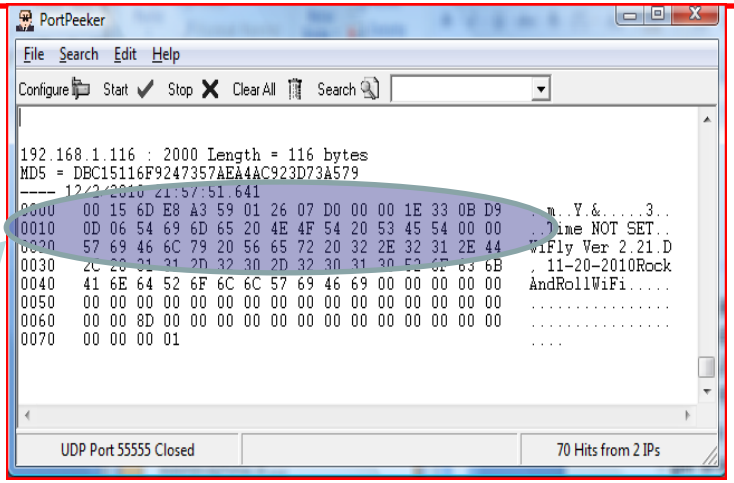


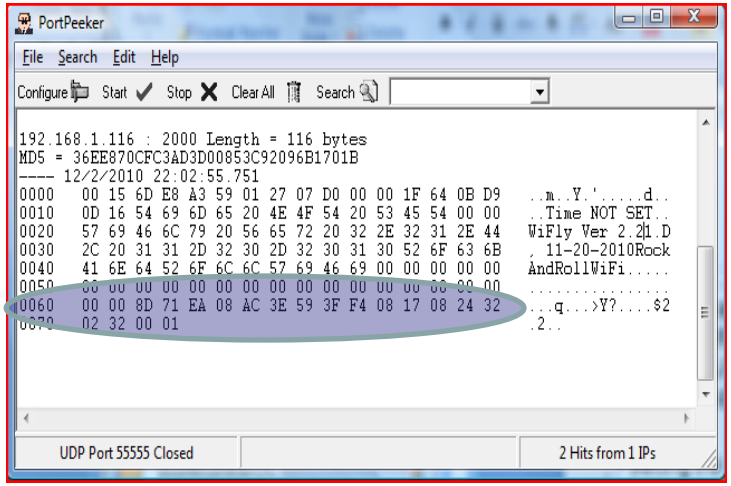


CONFIDENTIAL

Lab 1: UDP Broadcast

- **Module Sends UDP Broadcast at Specified Intervals**
- **UDP Broadcast Contains Information that Identifies Module on Network**
- **Set UDP Broadcast Interval**
  - Enter command mode
    - **get broadcast** (observe current interval)
    - **set b i 3** (b=broadcast, i=interval)
    - **save & reboot**
  - Review UDP messages in PortPeeker
- **Enable Sensor Data in UDP Broadcast**
  - Enter command mode
    - **set q s 0xff** (set sensor mask)
    - **save** to make persistent
  - Reboot not required
  - Review UDP messages in PortPeeker
    - Sensor data highlighted



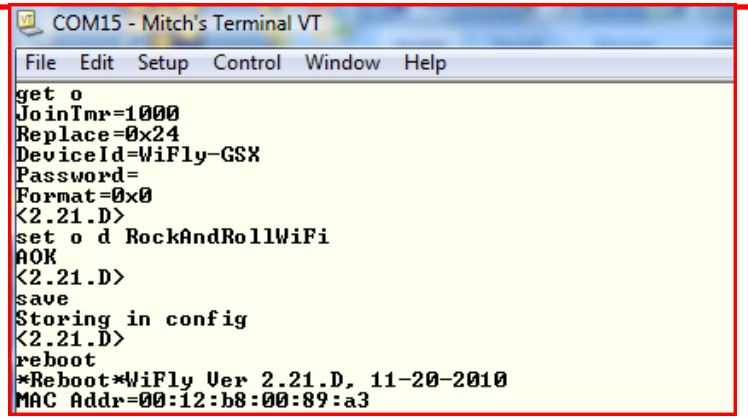


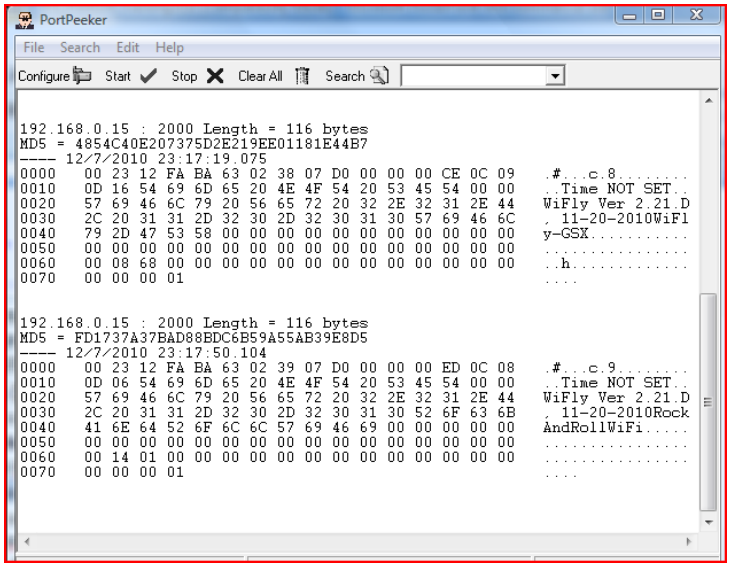
CONFIDENTIAL

Lab 1: Setting Device Name

- **Device Names Can Identify Products on Network**
- **Can Append Device ID to UDP Broadcast**
- **Set Device ID**
  - Enter command mode
    - **get option**
    - **set o d RockAndRollWiFi**(o=optional, d=deviceID)
    - **save & reboot**
  - Review UDP messages in PortPeeker
- **Set Broadcast UDP Port**
  - Enter command mode
    - **get broadcast**
    - **set b p 50000** (b=broadcast, p=port)
    - Save & reboot not required
  - Reconfigure PortPeeker to listen for UDP packets on port 50000
  - Review UDP messages in PortPeeker

TIP: UDP Broadcast on by Default
Set Interval to 0 to Turn It Off





CONFIDENTIAL

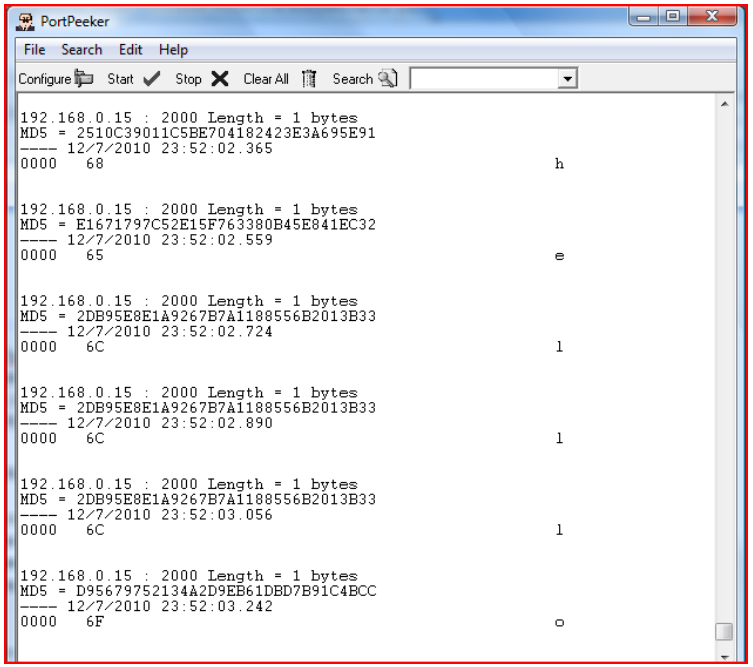
Lab 1: Sending UDP Packets

- **UDP Mode Not Enabled by Default**
- **Enable UDP by Setting Remote Host, Port & Protocol**
  - Enter command mode
    - **factory R**
    - Associate with AP
    - **set ip host** <*address*>
    - **set ip remote 50000**
    - **set ip proto 1** (IP protocol bitmask; 1 = UDP)
    - **set comm timer 1000** (try 10, see the change)
    - **get ip**
    - **save & reboot**
  - Type characters; they appear in PortPeeker

Bit Position	Protocol
0	UDP
1	TCP Server & Client (Default)
2	Secure (only receive packets with IP address matches the store host IP)
3	TCP Client only
4	HTTP client mode

TIP: IP Protocol Value Is a Bit Mask
You Can Enable Both TCP & UDP Messages

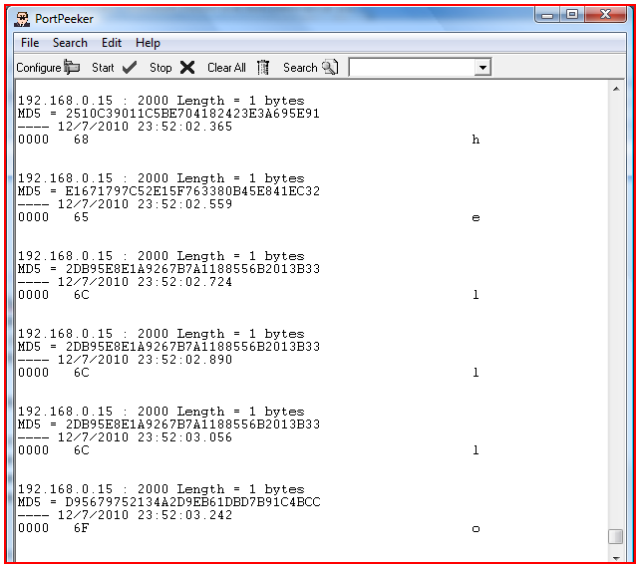
```
<2.21.D>
get ip
IF=UP
DHCP=ON
IP=192.168.0.15:2000
NM=255.255.255.0
GW=192.168.0.1
HOST=192.168.0.12:55555
PROTO=UDP,
MTU=1524
FLAGS=0x7
BACKUP=0.0.0.0
```



CONFIDENTIAL

Lab 1: UDP Auto Pairing Mode (Optional Slide)

- **Similar to Bluetooth Pairing, Module Can Store IP Addresses for Fast UDP Message Setup**
- **Example Requires 2 Modules**
- **Module 1: Clear Host IP & Port & Set Auto Pair Mode**
  - **$$$** (enter command mode)
  - **set ip host 0.0.0.0**
  - **set ip remote 2000**
  - **set ip local 2000**
  - **set ip flag 0x40**
  - **save & reboot**
- **Module 2: Set Module 1 Host IP & Port**
  - **$$$** (enter command mode)
  - **set ip host** <*module 1 address*>
  - **set ip remote 2000**
  - **set comm timer 1000**
  - **save & reboot**
- **Test System**
  - Type characters in module 2's terminal; they appear in module 1's terminal window
  - Type characters in module 1's terminal; they appear in module 2's terminal window



CONFIDENTIAL

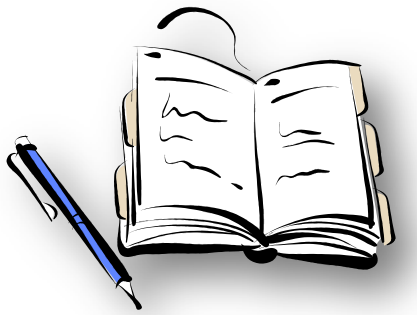
Lab 1: Conclusion

- RN-134-K or RN-174-K with Terminal Emulator & Serial Cable Provides Simple, Effective Development Environment
- Joining Networks Is Easy
- Use Broadcast UDP to Find Modules on Network Using Device Names & MAC Addresses
- Module Sends UART Data as UDP Packets when Associated with Network in UDP Mode

CONFIDENTIAL

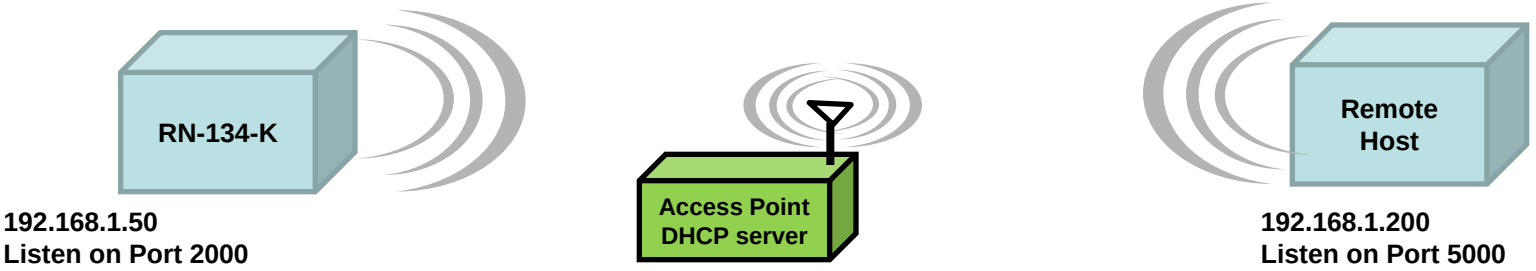
Lab 2: TCP

- **Objective**
  - Connect **from** module to remote host using TCP
  - Connect **to** module from remote host using TCP
  - TCP modes
  - Auto-connect features
  - Alternative GPIO functions
  - Event-based TCP packet forwarding
- **Prerequisites**
  - RN-134-K set up as in Lab 1
  - Module associated to access point (AP)
  - Computer associated to same AP
  - Telnet client (Tera Term)
  - PortPeeker application



CONFIDENTIAL

Lab 2: TCP Connections



TCP Connections Are Point to Point
Provide Reliable, Guaranteed, In Order Data Delivery
Also Known As Sockets

open 192.168.1.200 5000 ⟶

WiFly Module Opens TCP Connection

- Sensing applications
- Sending data to web server
- Data acquisition systems
- Fleet management

⟵ **open 192.168.1.50 2000**

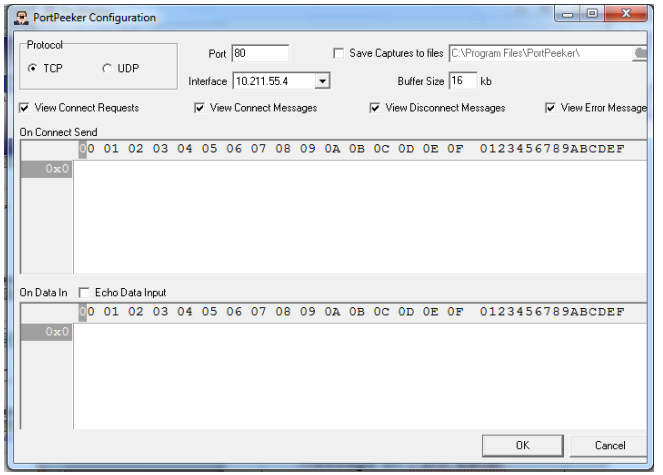
Remote Host Opens TCP Connection

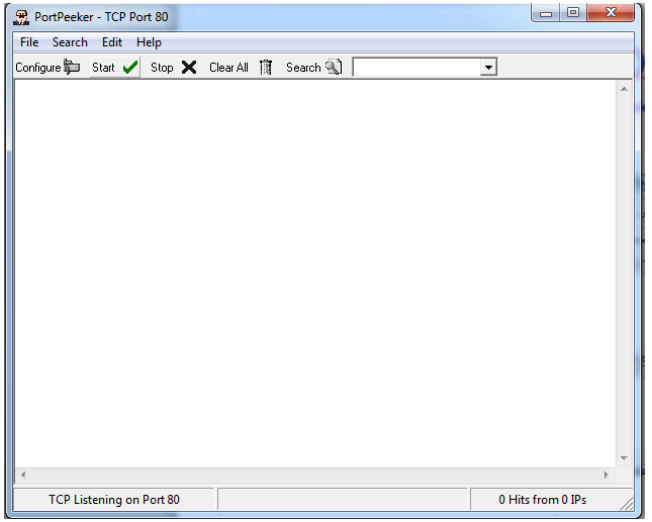
- Industrial controls
- Home automation
- Universal remotes

CONFIDENTIAL

Lab 2: Setup PortPeeker

- **Associate Computer with AP**
- **Launch PortPeeker**
- **Configure PortPeeker**
  - Click **Configure**
    (Note PC's IP address in Interface box)
  - Set port to 5000
    (port number matches remote port of WiFly module)
  - Set protocol to TCP
- **Click Start to Capture TCP Packets**

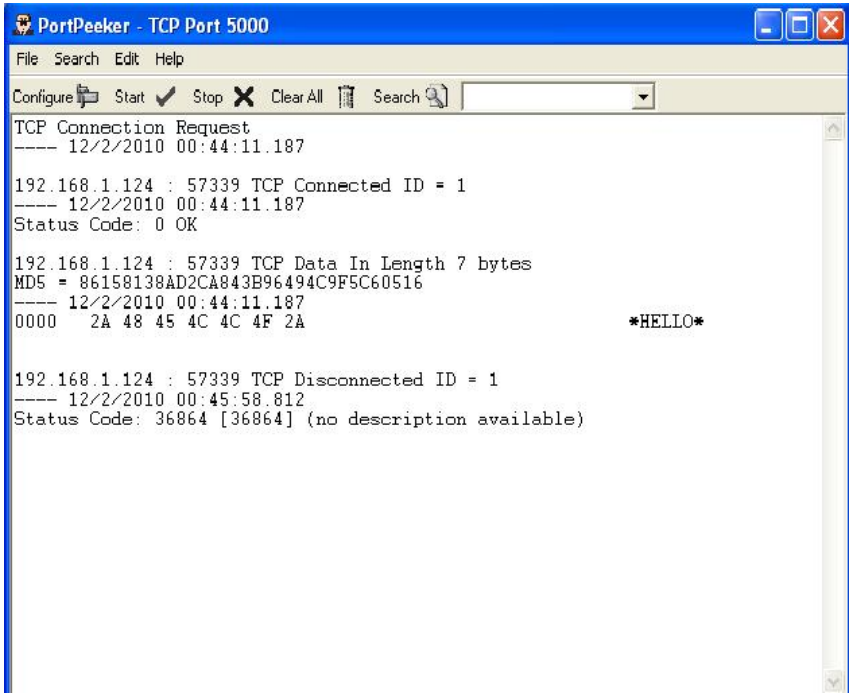




CONFIDENTIAL

Lab 2: Open TCP Connection from Module

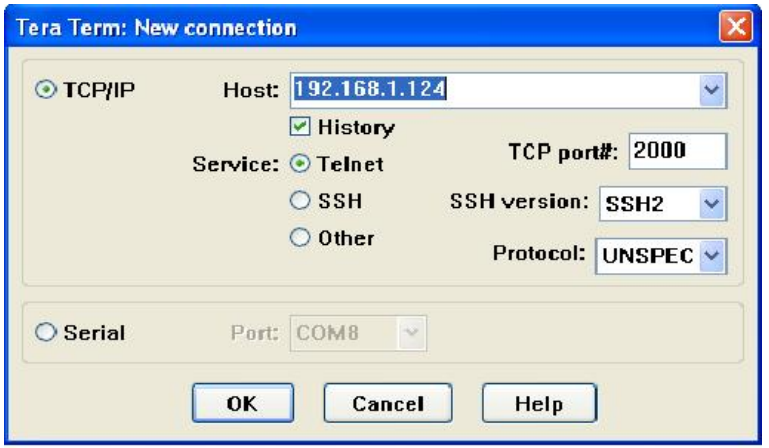
- **With Module Connected to PC over USB-Serial Cable, Open Tera Term on Serial COM Port**
- **Restore Module to Factory Defaults**
  - Enter command mode
  - **factory R**
  - Associate with AP
  - **save** & **reboot**
- **Open TCP connection**
  - **open** <*remote host address*> **5000**
  - *OPEN* shown on serial port (Tera Term window) & packet with *HELLO* on PortPeeker
- **Close TCP Connection**
  - Enter command mode
  - **close**
  - Close string *CLOS* displayed in Tera Term

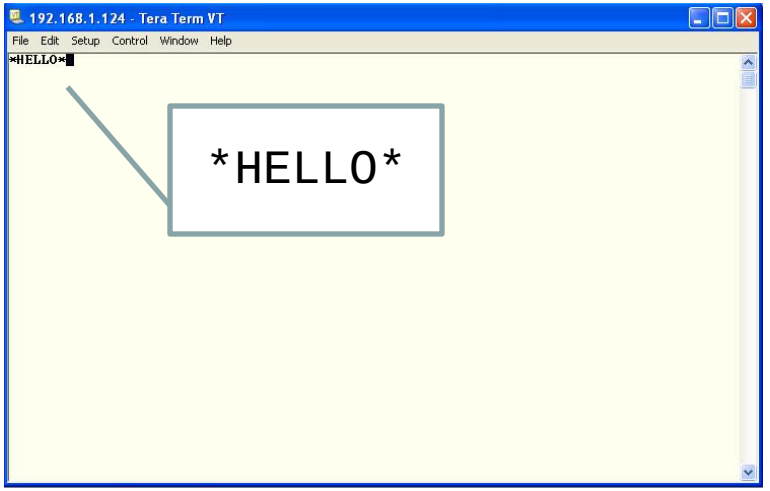

PortPeeker - TCP Port 5000
File Search Edit Help
Configure Start Stop Clear All Search
TCP Connection Request
---- 12/2/2010 00:44:11.187
192.168.1.124 : 57339 TCP Connected ID = 1
---- 12/2/2010 00:44:11.187
Status Code: 0 OK
192.168.1.124 : 57339 TCP Data In Length 7 bytes
MD5 = 86158138AD2CA843B96494C9F5C60516
---- 12/2/2010 00:44:11.187
0000 2A 48 45 4C 4C 4F 2A *HELLO*
192.168.1.124 : 57339 TCP Disconnected ID = 1
---- 12/2/2010 00:45:58.812
Status Code: 36864 [36864] (no description available)

CONFIDENTIAL

Lab 2: Connecting from Remote Host to WiFly module

- **In Command Mode, Obtain Module's IP Address**
  - **get ip**
- **Open Telnet Connection from PC Using Tera Term (Use Existing Instance)**
  - Click **File > New connection**
  - Select **TCP/IP**
  - Select **Telnet**
  - In **Host** field, type module's IP address
  - **TCP port#** is 2000 (default listening port)
  - Click **OK**
- ***HELLO* Message Shown in Telnet Window Indicating Successful TCP Connection**
- **Type in Telnet Window; Data Appears on Serial Port Window & Vice Versa**
- **Can Configure Module Remotely over Telnet by Entering Command Mode**





CONFIDENTIAL

Lab 2: TCP modes

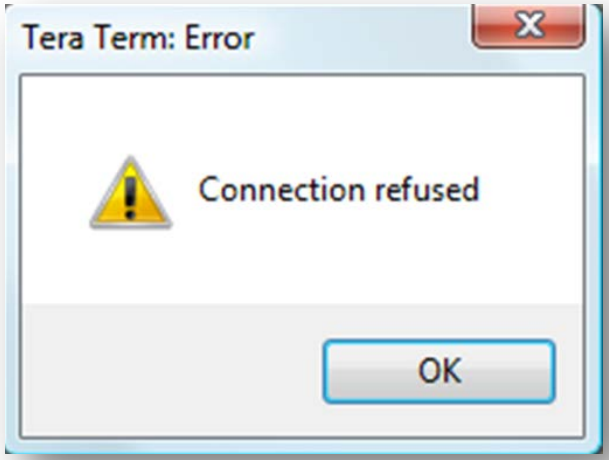
- **Module Supports Three TCP Modes**
  - TCP client & server mode
    - Default mode initiates & accepts TCP connections
    - Currently supports one active connection at a time
    - Concurrent TCP connections supported in future
  - TCP client ONLY mode
    - ONLY initiates TCP connections; cannot accept incoming connections
  - Secure mode
    - ONLY receives packets from host that matches stored host IP address

TIP: Refer to User Manual for More Details on TCP Modes

CONFIDENTIAL

Lab 2: TCP Client Mode

- **Set Up Module in TCP Client Mode**
  - **set ip proto 8**
  - **save & reboot**
- **Open New Telnet Connection to Module from Tera Term**
- **Second Connection Is Refused Indicating TCP_Client Mode Works Correctly**



CONFIDENTIAL

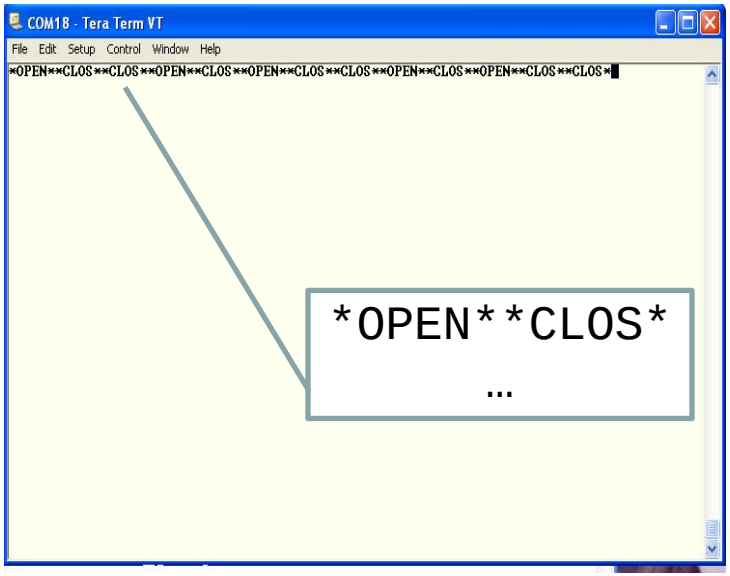
Lab 2: Auto-Connect Feature

- **Module Can Automatically Open TCP Connection to Remote Host on Power Up or Waking from Sleep**
- **Auto-Connect Controlled by autoconn Setting**
  - **set sys auto 1** // Attempts to open TCP connection immediately once only
  - **set sys auto** <*value*> // Attempts to open TCP connection every <*value*> seconds
  - **set sys auto 255** // Attempts to open TCP connection once & go back to sleep immediately // when connection is closed
- **Auto-Connect Requires Module to Store Remote Host's IP Address & Port #**
  - **set ip host** <*host IP address*>
  - **set ip remote** <*port*>
- **Once TCP Connection Is Opened, It Can Be Closed in Several Ways**
  - **close** command
  - Idle timer
  - Remote host
- **Idle Timer Closes TCP Connection after Preset # of Seconds of No Activity (No Tx or Rx) on the TCP Link**
  - **set com idle** <*value*> //Closes the TCP connection after <*value*> seconds of inactivity

CONFIDENTIAL

Lab 2: Auto Connect Feature (Timers)

- **Module Attempts a TCP Connection Every 10 seconds, Drops Connection after 3 seconds Inactivity**
  - **set ip host** <*address*>
  - **set ip remote 5000**
  - **set sys auto 10**
  - **set comm idle 3**
  - **save**
  - **reboot**
- **PortPeeker: Connection Opens & Closes**
- **Tera Term: Open & Close Strings Shown when Each Connection Opens & Closes**



CONFIDENTIAL

Lab 2: Alternative GPIO Functions

- **Firmware Uses GPIO 4, 5 & 6 to Blink Evaluation Board's Status LEDs (See Section 2.4 in User Manual for Standard LED Function)**

GPIO	Function	Description
4 (GRN)	Output	High once associated, authenticated & has IP address.
5 (RED)	Input	Set high to trigger TCP connection, low to disconnect.
6 (YLW)	Output	High when connected over TCP, low when disconnected.

- **Microcontroller Opens or Closes TCP Connection to Stored Remote Host by Driving GPIO5 High or Low**
  - This setup requires a hardware configuration that is not part of this lab
- **Microcontroller Can Monitor TCP Connection Status by Reading GPIO6**
  - High = Connected
  - Low = Not Connected

CONFIDENTIAL

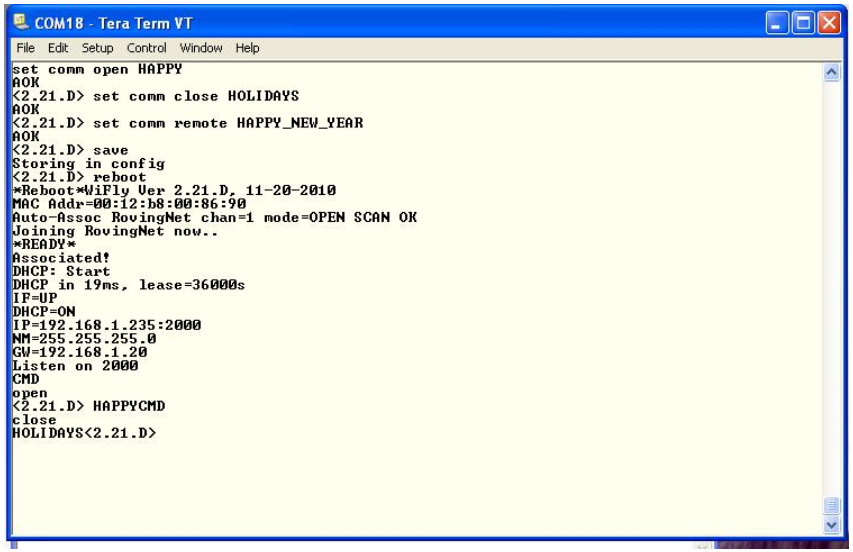
Lab 2: Alternative GPIO Functions

- **Enable Alternative Functions**
  - **set wlan ssid** <*string*>
  - **set sys iofunc 0x70**
  - **save**
  - **reboot**
  - Evaluation board LEDs do not turn on
- **After Module Associates with AP**
  - Associate with AP
  - **save & reboot**
  - Green LED goes on (GPIO4)
- **Connect/Disconnect TCP Connection**
  - Enter command mode (**$$$**)
  - **open** <*address*><*value*>
  - Red LED blinks & connection closed because RN-134-K board's GPIO5 pulled to GND
  - Enter command mode (**$$$**)
  - **leave** // disassociate from AP
  - Green LED goes OFF

CONFIDENTIAL

Lab 2: Setting Comm Strings

- **Microcontroller Can Look for UART comm Strings as Indication of TCP Connection Status**
  - Factory reset
  - **reboot**
  - Associate with AP
  - **set ip host** <*address*>
  - **set ip remote 5000**
  - **set comm open HAPPY**
  - **set comm close HOLIDAYS**
  - **set comm remote HAPPY_NEW_YEAR**
  - **save & reboot**
  - Enter command mode
  - **open**
  - See open string in Tera Term
  - See remote string in PortPeeker
  - Enter command mode
  - **close**
  - See close string in Tera Term



Tip: Microcontroller Can Read UART Open & Close Strings to Determine TCP Connection Status

CONFIDENTIAL

Lab 2: Forwarding TCP packets

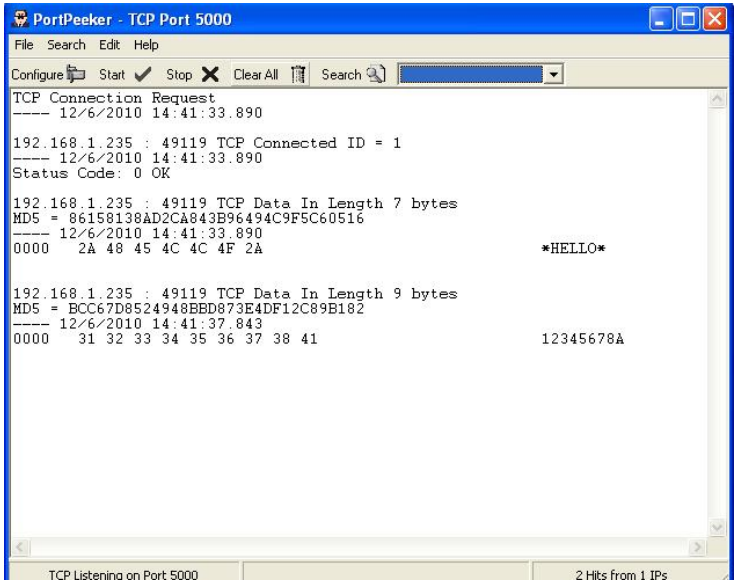
- **When Data Is Written to Module's UART, TCP Packets Forwarded Based On**
  - Flush timer
  - Flush size
  - Match character
- **TCP Packet Sent When Any of These Events Occur**
- **Parameters Logically ORed to Determine when TCP Packet Is Sent**
- **When Configured Correctly, Module Can Be Optimized for Low Latency or High Throughput**
  - Low latency: use lower flush timer value & flush size
  - High throughput: use higher flush timer value & flush size

Tip: Module Tries to Optimize Automatically for Bandwidth by Increasing Default Flush Size with Higher Baud Rates

CONFIDENTIAL

Lab 2: Forwarding TCP packets

- **Forwarding Packets Based on Flush Timer**
  - **set comm timer 1000**
  - **save**
  - **open**
  - Type text after TCP connection opens
  - After you stop typing, TCP packet is sent 1 second later
- **Forward Packets Based on Match Character**
  - **set c t 0** *(why do we send this command ?)*
  - **set comm match 65**
    - This parameter expects ASCII decimal character or HEX value of the match character (e.g., 65= Capital A)
  - **save**
  - **open**
  - Type 12345678A
  - TCP packet sent out after you type A character
  - Observe packet in PortPeeker
- **What Do You Learn from Using 'get c' Command?**


PortPeeker - TCP Port 5000
File Search Edit Help
Configure Start Stop Clear All Search
TCP Connection Request
---- 12/6/2010 14:41:33.890
192.168.1.235 : 49119 TCP Connected ID = 1
---- 12/6/2010 14:41:33.890
Status Code: 0 OK
192.168.1.235 : 49119 TCP Data In Length 7 bytes
MD5 = 86158138AD2CA843B96494C9F5C60516
---- 12/6/2010 14:41:33.890
0000 2A 48 45 4C 4C 4F 2A *HELLO*
192.168.1.235 : 49119 TCP Data In Length 9 bytes
MD5 = BCC67D8524948BBD873E4DF12C89B182
---- 12/6/2010 14:41:37.843
0000 31 32 33 34 35 36 37 38 41 12345678A
TCP Listening on Port 5000
2 Hits from 1 IPs

CONFIDENTIAL

Lab 2: Conclusion

- **Module Can Open TCP Connection to Remote Host & Accept Incoming Connections from Remote Host**
- **Auto-Connect Automatically Opens TCP Connection**
- **Idle Timer Can Automatically Close TCP Connection**
- **Alternative GPIO Functions Allow Microcontroller to Control & Monitor TCP Connections**
- **comm open, close & remote Strings Can Indicate TCP Connection Status**
- **TCP Packets Forwarded Based On**
  - Packet size
  - Match character
  - Flush timer

CONFIDENTIAL

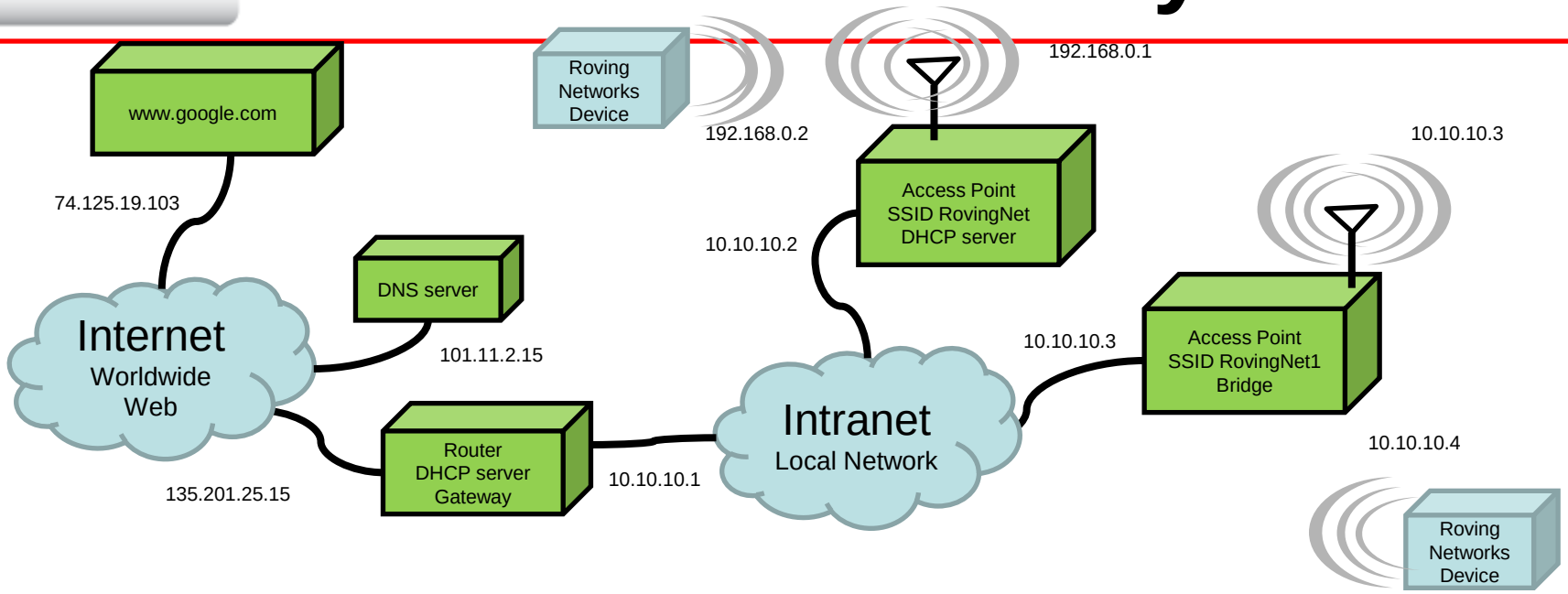
Lab 3: Association/Roaming & FTP

- **Objective**
  - Wake & sleep timers
  - Auto join
  - Roaming configuration (Linkmon/IP flags)
  - FTP

- **Prerequisites**
  - User has completed Labs 1 & 2
  - Evaluation board & computer set up as described in Lab 1

CONFIDENTIAL

Lab 3: Where in the World Wide Web are you?

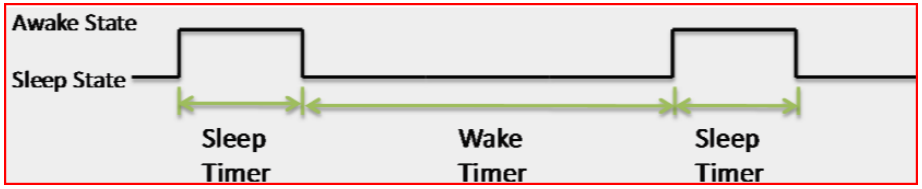


- **Module Associates with AP Based on SSID**
  - Password required depending on security
  - Multiple security modes
  - Multiple AP with same SSID and/or password
- **Each Wi-Fi Device Must Have Unique IP Address**
  - Provided by DHCP server
  - Gateway bridges multiple networks, typically Internet with Intranet
- **Dynamic Name Service (DNS)**
  - Maps URL (www.google.com) to an IP Address 74.125.19.103

CONFIDENTIAL

Lab 3: Wake & Sleep Timers

- **Several Options to Wake Module**
  - FORCE WAKE Signal
  - Sensors
  - Internal Timers



- **Restore Factory Default Parameters & Training AP**
  - Enter command mode
  - **factory R**
  - Associate module with AP
  - **save** & **reboot**
- **Set Wake Timer: # Seconds in Deep Sleep before Wake Up**
  - **set sys wake 10**
- **Set Sleep Timer: # Seconds before Entering Deep Sleep**
  - **set sys sleep 5**
  - **save** & **reboot**
  - LEDs cycle on & off (except blue),
  - Observe module reboot on wake up in Tera Term

TIP: Do Not Set Sleep Timer to Less than 2 Seconds or It Is Hard to Go into Command Mode & Reconfigure Module before It Sleeps Again

CONFIDENTIAL

Lab 3: Join Modes

- **Useful for Module to Associate with Network Automatically**
- **Association Controlled with join Command or join Parameter Setting**
- **Turn Off Auto-Join & Join Manually**
  - Enter command mode
  - **factory R & reboot**
  - Associate module with AP
  - **set wlan join 0**
  - **save & reboot**
  - Enter command mode
  - **Join**
  - Modules associates with AP
- **Auto-Associate with Any Open-Security AP**
  - **set wlan ssid** <*string*>
  - **set wlan join 2**
  - **set wlan auth 0**
  - **save & reboot**
  - Module attempts to join any open network (no security)

TIP: If Network is Secure, Set Pass Phrase with "set wlan pass <*password*>" before Joining Network

Value	Policy
0	Manual. Do not join automatically.
1	Attempt to join the AP that matches the stored SSID, pass phrase & channel. Channel can be set to 0 for scanning. (Default)
2	Join any AP with security matching the stored authentication mode. This setting ignores the stored SSID and searches for the AP with the strongest signal. The channels searched can be limited by setting the channel mas.
3	Reserved. Do not use.
4	Create an ad hoc network using the stored SSID, IP address & netmask. You must set the channel.

```
<2.21.D>
reboot
*Reboot*WiFly Ver 2.21.D, 11-20-2010
MAC Addr=00:12:b8:00:89:a3
*READY*
Best=05B403872286 on 6
Auto-Assoc 05B403872286 chan=6 mode=OPEN SCAN OK
Joining 05B403872286 now..

SCAN:Found 3
Num             SSID   Ch  RSSI   Sec     MAC Address      Suites
 1               FishNet 02 -61 WPA2PSK 00:23:12:fa:ba:63 AESM-AES  3100    0
 2                  RiFi 06 -82 WPA2PSK 00:23:69:b3:f7:24 AESM-AES  3104    0
 3          05B403872286 06 -87    Open 00:e0:98:fd:f4:e8   6104    0
Best=RovingNet on 1
Auto-Assoc RovingNet chan=1 mode=OPEN SCAN OK
Joining RovingNet now..

SCAN:Found 3
Num             SSID   Ch  RSSI   Sec     MAC Address      Suites
 1            RovingNet 01 -47    Open 00:15:6d:e8:a3:59   2100    0
 2           abbypolly5 01 -87     WEP 00:1d:7e:2c:ea:10   1104    4
 3               FishNet 02 -59 WPA2PSK 00:23:12:fa:ba:63 AESM-AES  3100    0
Associated!
DHCP: Start
DHCP in 23ms, lease=36000s
IP=UP
DHCP=ON
IP=192.168.1.176:2000
NM=255.255.255.0
GW=192.168.1.20
Listen on 2000
```

CONFIDENTIAL

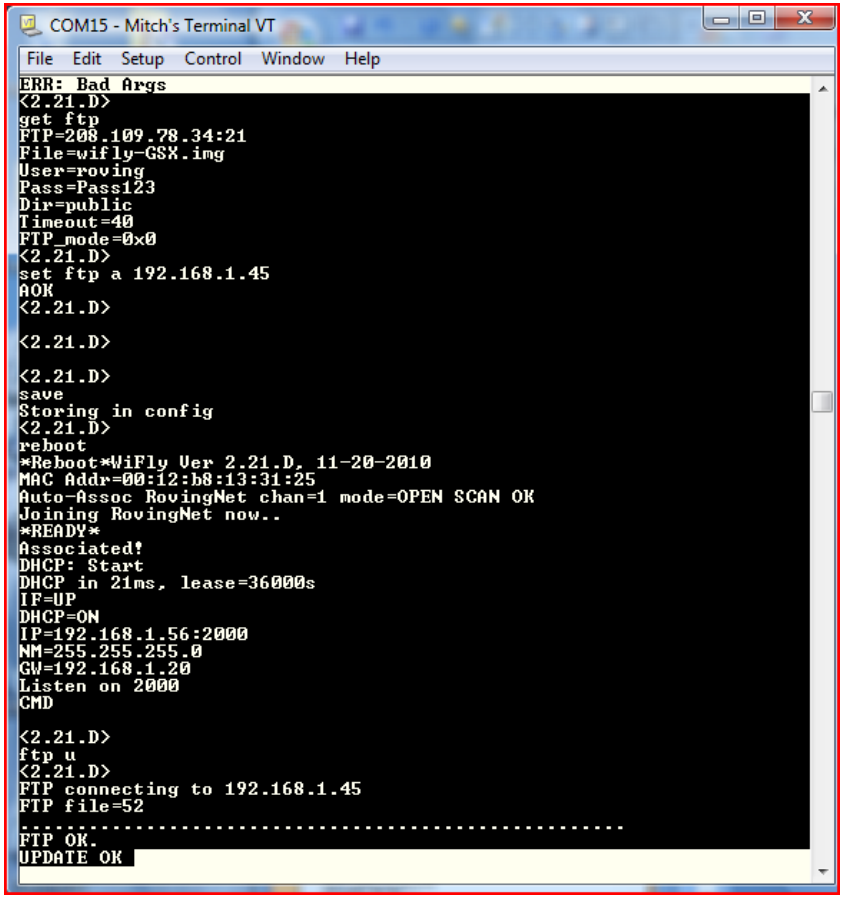
Lab 3: Roaming (Optional Slide)

- **Module Wakes, Searches for Aps, Connects, Off Loads Data & Returns to Sleep**
- **Used for Asset Tracking, Fleet Management & Remote Sensor Applications**
- **Combine Broadcast UDP, Wake Timers & Auto Join**
  - Enter command mode
  - **factory R & reboot**
  - **set broad interval 3**
  - **set opt device** *<string>*
  - **set wlan join 2**
  - **set wlan auth 0**
  - **set sys sleep 15**
  - **set sys wake 5**
  - **save & reboot**
- **Open PortPeeker to Receive UDP Broadcast Messages (Lab 1)**
- **Confirm Module's UDP Broadcast Message**
- **Move Module Near AP_SSID1 AP**
- **Move Module Near AP_SSID2 AP**
  - PortPeeker shows AP MAC address in broadcast UDP message change

CONFIDENTIAL

Lab 3: FTP Update (REQUIRES Internet Access)

- **Use Module's FTP Client to Update Firmware & Put/Get Data**
- **Default Username/Password Set to Roving Networks' FTP Server**
- **Associate to Internet-Connected Network & Use "ftp update" Command**
- **Use Local FTP Server**
  - Enter command mode
  - **factory R**
  - Associate module with AP
  - **save** & **reboot**
- **Update Firmware**
  - Enter command mode
  - **ftp update**
  - **ver**
  - **reboot**
  - Enter command mode
  - **Ver**

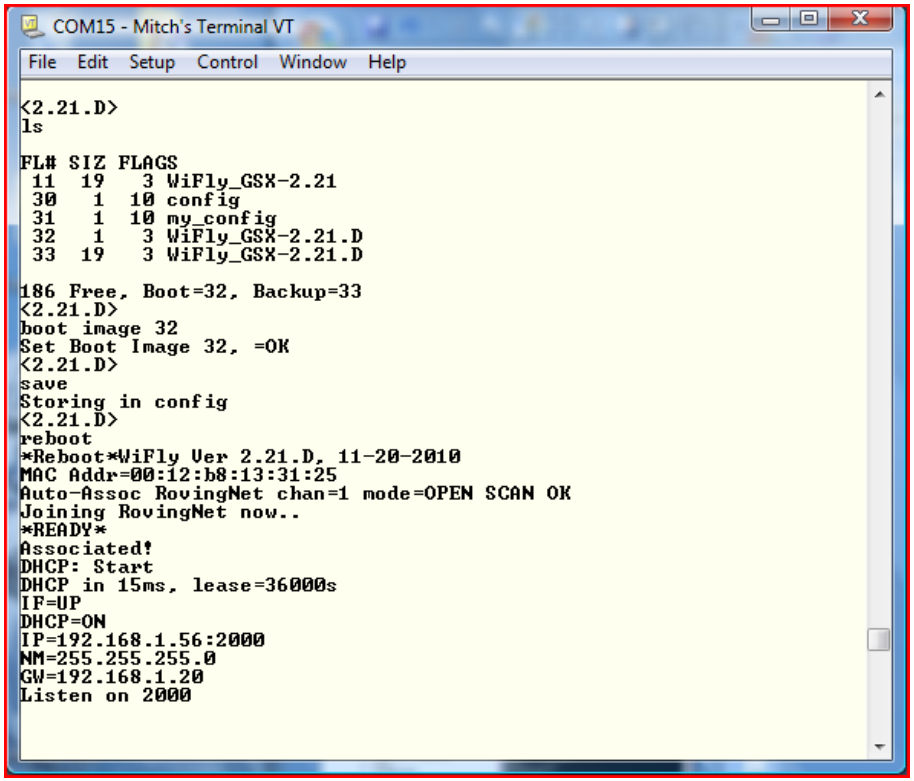


TIP: After Downloading New Firmware, Restore Module to Factory Defaults Before Using It

CONFIDENTIAL

Lab 3: Setting Firmware Boot Image

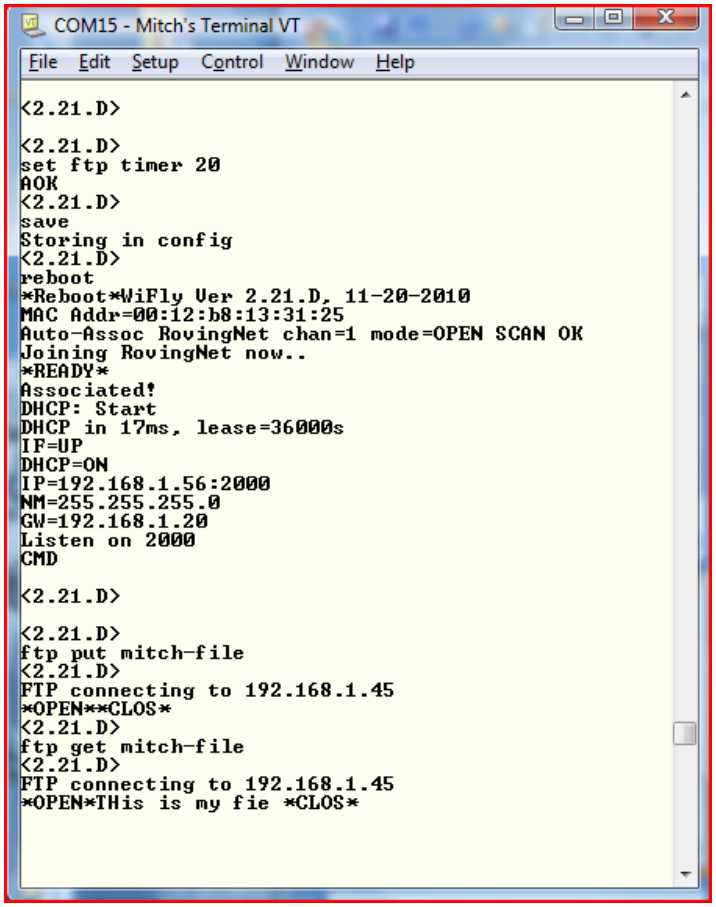
- **Firmware Stored in Embedded Flash Memory**
- **Boot Image is Firmware Version Module Is Currently Running**
- **After Successful Update, Boot Image Changes to New Firmware File**
- **Change Boot Image**
  - Enter command mode
- **View Files in Flash**
  - Enter command mode
  - **ls**
- **Change Boot Image**
  - Enter command mode
  - **boot image** <*value*>
  - **reboot**



CONFIDENTIAL

Lab 3: FTP put & get

- **FTP Client Can Stream Files to/from FTP Server**
  - Useful in data logger applications
- **FTP Servers Can Accept Multiple Clients Concurrently**
- **Configure FTP Setup**
  - Enter command mode
  - **factory R & reboot**
  - Associate module with AP
  - **set ftp address** <*address*> (e.g., ftp svr addr)
  - **set ftp user** <*string*> (e.g., roving)
  - **set ftp pass** <*string*> (e.g., Pass123)
  - **set ftp dir** <*string*> (e.g., public)
  - **set ftp timer 20**
  - **save & reboot**
- **Create & Read File on Server**
  - Enter command mode
  - **ftp put** <*string*>
  - Type characters, wait until *CLOS* shown
  - **ftp get** <*string*>



CONFIDENTIAL

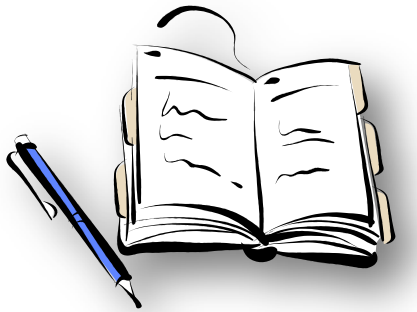
Lab 3: Conclusion

- Sleep & Wake Timers Allow Module to Deep Sleep to Save Power & Periodically Connect to Network
- Roaming Allows Module to Connect to AP with Strongest Signal that Matches SSID or Authentication Mode
- Use FTP to Update Firmware
- Use FTP put & get Commands to Transfer Files
- FTP put Combined with Sleep/Wake/Roaming Useful for Data Logging Applications

CONFIDENTIAL

Lab 4: HTTP Client

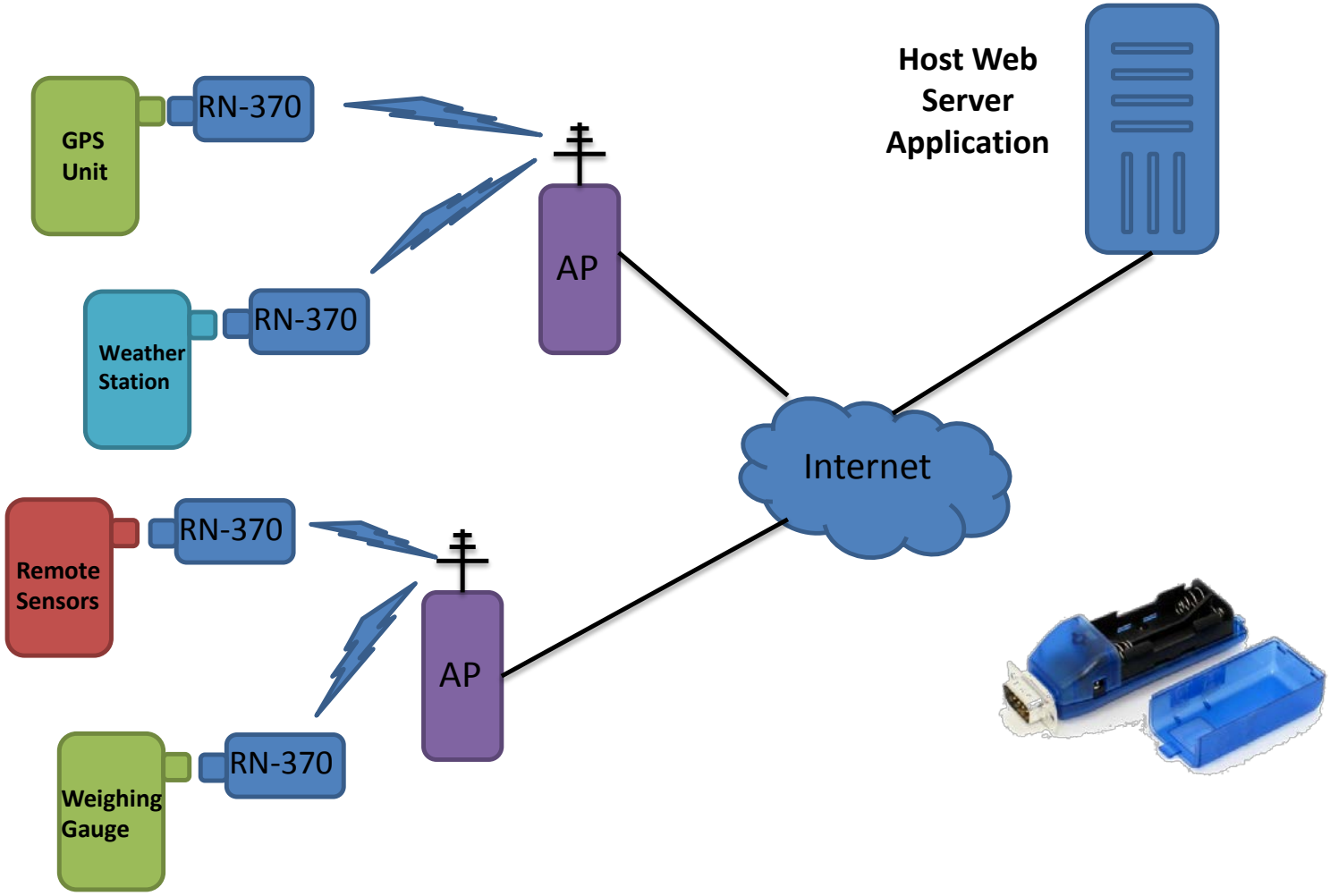
- **Objective**
  - Post data to web server
    - Uses built-in feature
    - Does not require external processor
  - Configure HTTP client mode
  - Periodically send sensor data web server
  - Wake on UART data



- **Prerequisites**
  - Hardware same as in previous labs
  - Module associated to Access Point (AP) with Internet connectivity
  - Tera Term running on PC
  - Web server configured to accept HTTP messages (Roving Networks Website)

CONFIDENTIAL

Lab 4: Solutions Architecture



CONFIDENTIAL

Lab 4: Enabling HTTP Client Mode

- **HTTP Client Mode Disabled by Default**
  - To enable use **set ip proto 18** command
- **Module Connects to Web Server Using the IP Address or URL**
- **Web Server Listens on Port 80 (Default) for Incoming Connections**
- **For Each Request**
  - Web server responds with **200 OK**
  - Closes the connection

CONFIDENTIAL

Lab 4: Auto-Posting Sensor Data

- **In HTTP Client Mode, Module Sends Request Message**
  - GET /server.php?value=0F300000111122223333444455556666777¥n¥n
  - Request message includes comm remote string & sensor readings
- **Configure HTTP Client Mode & Request Message**
  - Go into command mode
  - Associate the module with AP
  - **set ip proto 18** // Enable HTTP & TCP protocols
  - **set ip host 0** // Set IP address if known
  - **set dns name www.rovingnetworks.com** // Set DNS name if not
  - **set ip remote 80** // Standard web server port
  - **set comm remote GET$/server3.php?value=** // $ is replaced by space character
  - **set q sensor 0xff** // Sample all sensors inputs
  - **set option format 7** // Send header & sample sensor data
  - **save & reboot**
  - Enter command mode
  - **open**

Format

2 Bytes GPIO	Chan 0	Chan 1	Chan 2	Chan 3	Chan 4	Chan 5	Chan 6	Chan 7
0F30	0000	1111	2222	3333	4444	5555	6666	7777

CONFIDENTIAL

Lab 4: Web Server

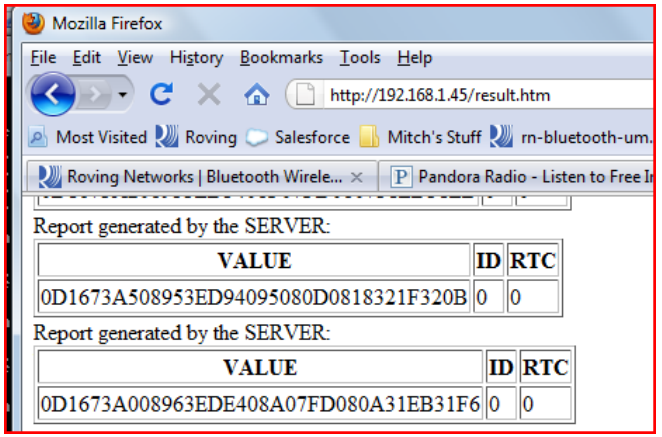
- **Open Web Browser**
  - The PC must be associated with your AP connected to the internet
- **In Address Bar, Type** www.rovingnetworks.com/result.htm
  - Scroll to bottom of log to see data
  - All module data looks the same

*OPEN*HTTP/1.1 200 OK
Date: Fri, 19 Nov 2010 19:24:07 GMT
Server: Apache
X-Powered-By: PHP/5.2.13
Connection: close
Content-Type: text/html

Server accepted values

ID: 0
VALUE: **0D16CF2907ED3EB640AB07E607F4321C3219**
RTC: 0

CLOS GPIO values Sensor Data


Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://192.168.1.45/result.htm
Most Visited Roving Salesforce Mitch's Stuff rn-bluetooth-um...
Roving Networks | Bluetooth Wirele...
Pandora Radio - Listen to Free I
Report generated by the SERVER:
VALUE ID RTC
0D1673A508953ED94095080D0818321F320B 0 0
Report generated by the SERVER:
VALUE ID RTC
0D1673A008963EDE408A07FD080A31EB31F6 0 0

CONFIDENTIAL

Lab 4: Add Device Name & RTC to Sensor Data

- **Append Device ID & RTC Value to Sensor Data so Server Can Identify It**
  - *Device String*: Appends **&id=**<*value*>, where <*value*> is device ID string set with **set opt device** <*string*> command
  - *Real-Time Clock*: Appends **&rtc=**<*time*>, where <*time*> is real-time clock value in message as 32-bit HEX value in format aabbccddeeff
- **Turn Off Auto Connect**
  - Go into command mode
  - Set sys auto 0
  - Save & reboot
- **Append Device Name & RTC**
  - Go into command mode
  - **set option device** <string>
  - **time** // Get network time
  - **set option format 31**
  - **save & reboot**
- **Post Data**
  - Go into command mode
  - **open**

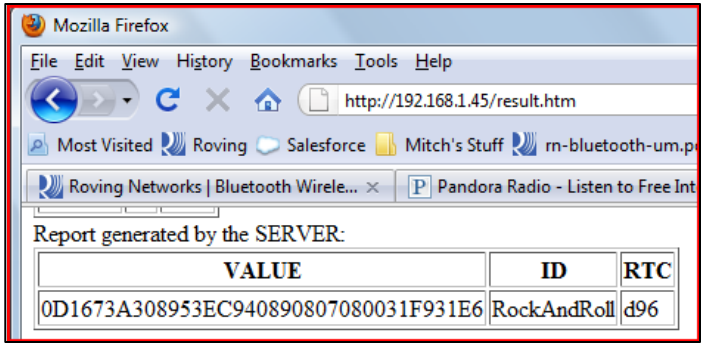
Tera Term Output

*OPEN*SEND-WEBPOST
HTTP/1.1 200 OK
Date: Mon, 06 Dec 2010 17:56:28 GMT
Server: Apache
X-Powered-By: PHP/5.2.13
Connection: close
Content-Type: text/html

Server accepted values
ID: servertest
VALUE: 0D16CF2908043E8540200801080432363 23A
RTC: 3ad82
CLOS

Device ID

Real Time Clock



CONFIDENTIAL

Lab 4: Auto-Posting UART Data

- **Module Can Wake on Receiving UART Data, Associate with AP & Send Request Message Containing the UART Data**

factory R & reboot	
Associate module to AP	
set ip proto 18	// set HTTP client mode
set ip host 0	// IP address of web server
set dns name www.rovingnetworks.com	// OR DNS name
set ip remote 80	// Web server port
set comm remote GET$/server3.php?value=	// Set request message header
set uart mode 2	// Automatically connect using trigger mode
set sys trigger 1	// Wake up on uart RX data
set sys sleep 10	// Put WiFly module to sleep after 10 seconds
set option format 1	// Sends out HTTP header
set comm timer 2500	// Allows multiple keystrokes per request
save & reboot	

- **In Tera Term, Type Characters to Wake Module, Associate to AP & Send Data as HTTP Message to Web Server**

NOTE: You Cannot Send both Sensor & UART Data in Same Request Message

CONFIDENTIAL

Lab 4: Auto-Posting Serial Data

- **When Serial UART Data Arrives, Module Auto-Connects to Web Server & Sends**

GET /server3.php?value=<*user's serial data*> **¥n¥n**

OPEN*SEND-WEBPOST
HTTP/1.1 200 OK
Date: Mon, 06 Dec 2010 18:25:36 GMT
Server: Apache
X-Powered-By: PHP/5.2.13
Connection: close
Content-Type: text/html
**Server accepted values
**
**ID: 0
**
VALUE: oving **Data with first byte missing**
RTC: 0
CLOS

NOTE: First Data Byte Dropped because Module Must Initialize before Sending Data over Wireless Interface

To Avoid This Issue, Module Should Wake on CTS Signal Using set sys trigger 2 or Send First Byte Twice

CONFIDENTIAL

Lab 4: Conclusion

- **Module Supports HTTP Client Mode Natively**
- **When Configured, Module Can Append**
  - GPIO values
  - Sensor data
  - Real-time clock
  - Device name
  - UART data
- **Module Can Wake Up on UART Data**
  - May result in dropping first byte
  - Waking up on CTS is better option

Lab 5: Access Point Mode

- **Advantages**
  - Enables Android devices to talk to modules without infrastructure
  - Runs DHCP server
  - Supports up to 10 clients
  - Supports routing between clients
  - Supports WPA2-AES personal security

CONFIDENTIAL

Lab 5: Creating a Default AP Network

- **Download Firmware Supporting AP Mode via FTP**
  - RN-131: **ftp update wifly-241.img**
  - RN-171: **ftp update wifly7-241.img**
  - RN-370: **ftp update wiflyA-241.img**
- **Install Jumper at J6 to Enable AP Mode in Hardware**
  - SSID: WiFlyAP-*XX*, where *XX* is last two bytes of MAC address
  - Channel: 1
  - DHCP server: Enabled
  - IP address: 1.2.3.4
  - Netmask: 255.25.5255.0
  - Gateway: 1.2.3.4

CONFIDENTIAL

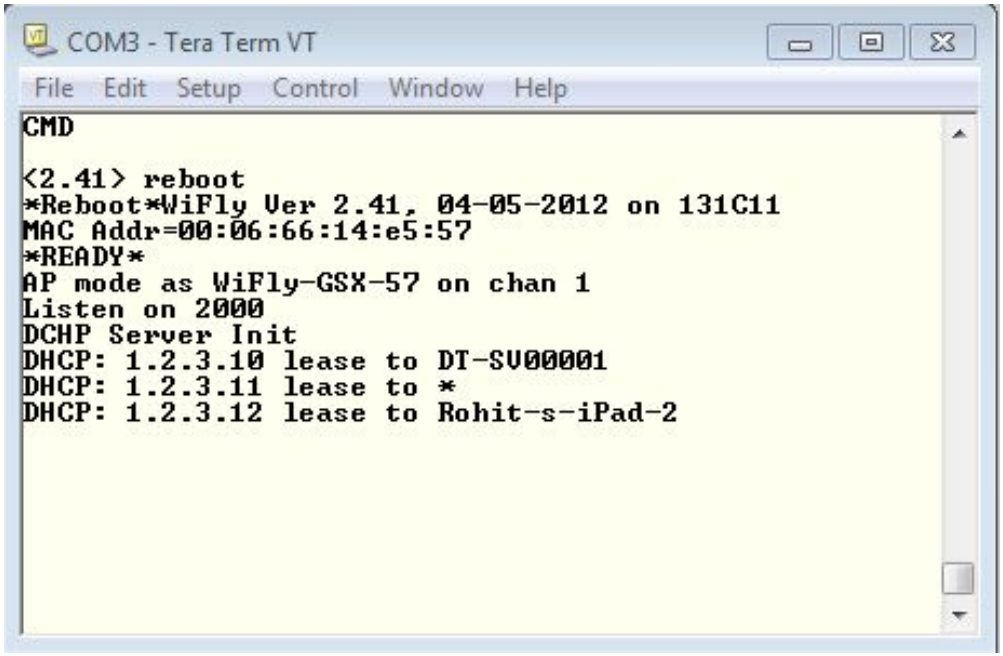
Lab 5: Create Custom AP Network in Software

- **Create Custom AP Network with User-Defined Settings**
  - **set wlan join 7** // Create AP mode network
  - **set wlan channel** <*value*> // Specify channel to create // network
  - **set wlan ssid** <*string*> // Set up network SSID
  - **set ip dhcp 4** // Enable DHCP server
  - **set ip address** <*address*> // Specify IP address
  - **set ip net** <*address*> // Specify subnetmask
  - **set ip gateway** <*address*> // Spcify gateway
  - **save** // Store settings
  - **reboot** // Reboot module in AP mode

CONFIDENTIAL

Lab 5: Connect to AP Network Created by Module

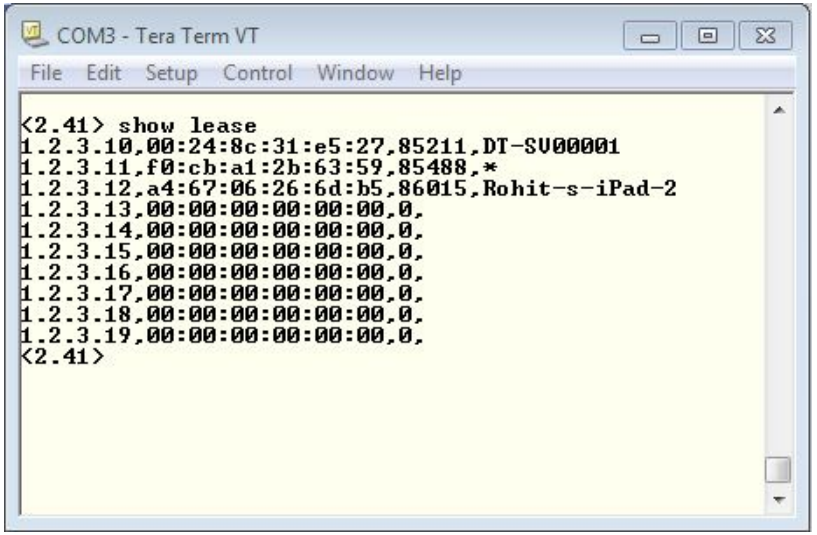
- From PC/Mobile Phone/Tablet, Connect to Module-Created Network
- Module Displays Client's Device Name

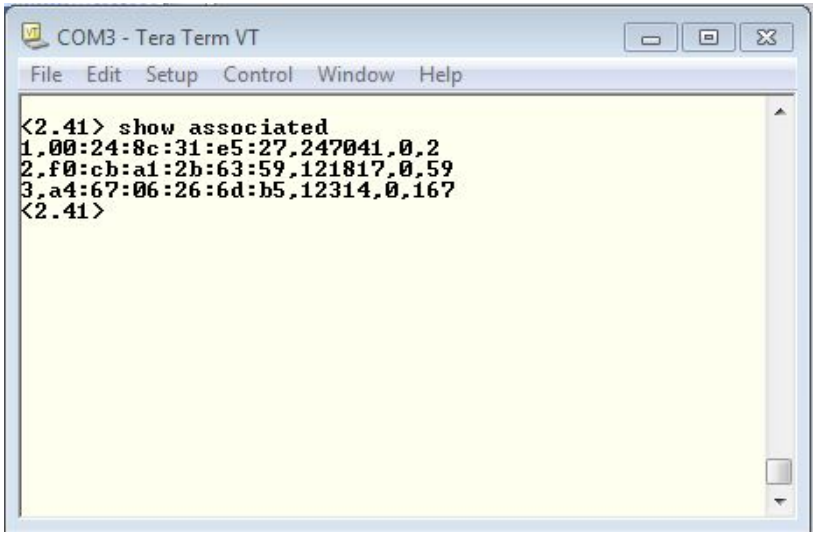


CONFIDENTIAL

Lab 5: View Associated Devices & Lease Times

- View Device Lease Times
  - show lease
- View List of Connected Devices
  - show associated





CONFIDENTIAL

Wi-Fi Training Session

Questions

CONFIDENTIAL